Power Analysis Part III

Cryptographic Hardware for Embedded Systems
ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading

- This lecture covers a portion of Chapter 4 and a very small portion of Chapter 5 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al., 2007, ISBN-13: 978-0-387-30857-9, ISBN-10: 0-387-30857-1, e-ISBN-10: 0-387-38162-7.
  - Specifically, sections 4.4, 5.1 and 5.2 are covered

Question Answered by This Lecture

- How specifically are different power traces gathered and what is their design in order to reveal the information claimed to have been learned?

8 key bits at a time

Power Analysis

- Recall that $P_{total} = P_{op} + P_{data} + P_{el.\ noise} + P_{const}$
- Note that P_{const} is a constant and we can use the same assembly instruction or operation so that P_{op} is also a constant
- Thus, the first component to model is electrical noise ($P_{el.\ noise}$)
- The next component to model is data dependent power (P_{data})
- Therefore, we need power traces to isolate each

Data Dependent Energy Consumption / Power

- Consider a single assembly instruction which loads a byte from on-chip memory to a register
  - Note we assume the closest level – Level 1 or L1 – of on-chip memory
  - Also notice that we are not varying the instruction at all
  - Finally, note that we assume byte-addressable memory (which may not be supported in modern 64-bit processors including those used in embedded devices!)
- Vary the eight bit memory data value among all 256 possible values
- 200 measurements for each value = 256* 200 = 51,200 total measurements
  - Note that for the data value of 0b00000000 = 0x00, there are only 200 measurements; thus, to obtain 10,000 power measurements for this case, an additional 9,800 must be taken

Plain Key

Operation Dependent Energy Consumption / Power

- Case 1: unpipelined single issue processor, e.g., microcontroller
  - Only one operation is underway at any point in time
  - Isolation of the operation-dependent power based on time of execution

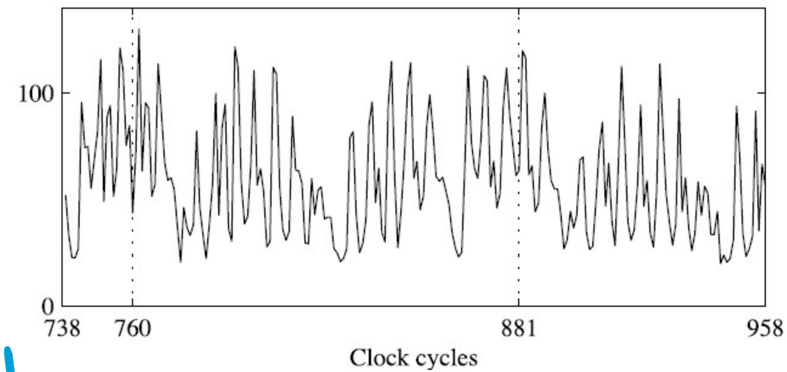

Figure 5.3. The sequence of AddRoundKey, SubBytes, and ShiftRows operations.

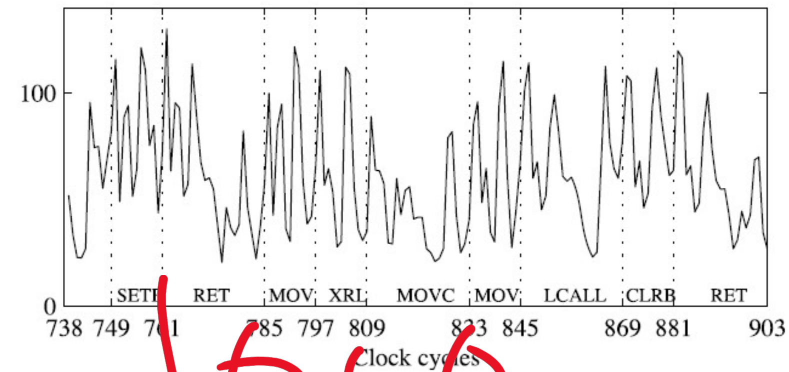

Figure 5.4. The annotated sequence of AddRoundKey, SubBytes, and ShiftRows operations.

```
LCALL SET_ROUND_TRIGGER
MOV A,ASM_input + 0       ; load a0
XRL A,ASM_key + 0         ; add k0
MOVC A,@A + DPTR          ; S-box look-up
MOV ASM_input, A          ; store a0
LCALL CLEAR_ROUND_TRIGGER
```

Figure 5.5. The sequence of assembly instructions that corresponds to Figure 5.4.

Operation Dependent Energy Consumption / Power

- Case 1: unpipelined single issue processor, e.g., microcontroller
  - Only one operation is underway at any point in time
  - Isolation of the operation-dependent power based on time of execution
- Case 2: pipelined single issue processor, e.g., 5 stages
  - E.g., Instruction Fetch (IF), Instruction Decode (ID), Execute (EX), Memory (MEM) and Write Back (WB); at any clock cycle there may be up to five instructions executing
  - Additional modeling and statistics are required beyond the scope of this course
- Case 3: pipelined multiple issue processor
  - Also beyond our scope
- Cases 4 and beyond: out of order, multicore, etc.
  - Even more complicated and also beyond our scope, but possible to analyze

Example

- A “case 1” processor operates on an 8-bit value where each bit is independent and uniformly distributed
- Assume that the value of the second bit is always the complement of the first bit in the experiments carried out
  - E.g., $0bX_7X_6X_5X_4X_3X_2X_10$ and $0bY_7Y_6Y_5Y_4Y_3Y_2Y_11$ where the first bit considered in our analysis is the case of the LSB = 0 and the second bit considered in our analysis is the case of the LSB = 1
  - The other 14 bits are independent and uniformly distributed
- P_{exp} consists of the energy consumed by the LSB
- $P_{switching}$ consists of the energy consumed by the rest of the bits

Example (continued)

- We have 51,200 power traces as computed already earlier
- Select the 25,600 traces with LSB = 1
- Figure 4.6 shows the resulting histogram at 362 ns

Correlation and Covariance

- Two points are correlated if they vary together in a related way
- Statistical measure: covariance
- *Cov(X,Y) = E[(X-E(X))*(Y-E(Y))] = E(XY) – E(X)E(Y)*
- Theoretical and empirical formulas:
- $\rho(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var(X)*Var(Y)}}$
- $r = \frac{\sum_{i=1}^{n}(x_i - \overline{x_i})*(y_i - \overline{y_i})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x_i})^2 * \sum_{i=1}^{n}(y_i - \overline{y_i})^2}}$
- As defined, the correlation coefficient ρ varies between -1 and 1, i.e., -1 ≤ ρ ≤ 1 and also thus -1 ≤ *r* ≤ 1

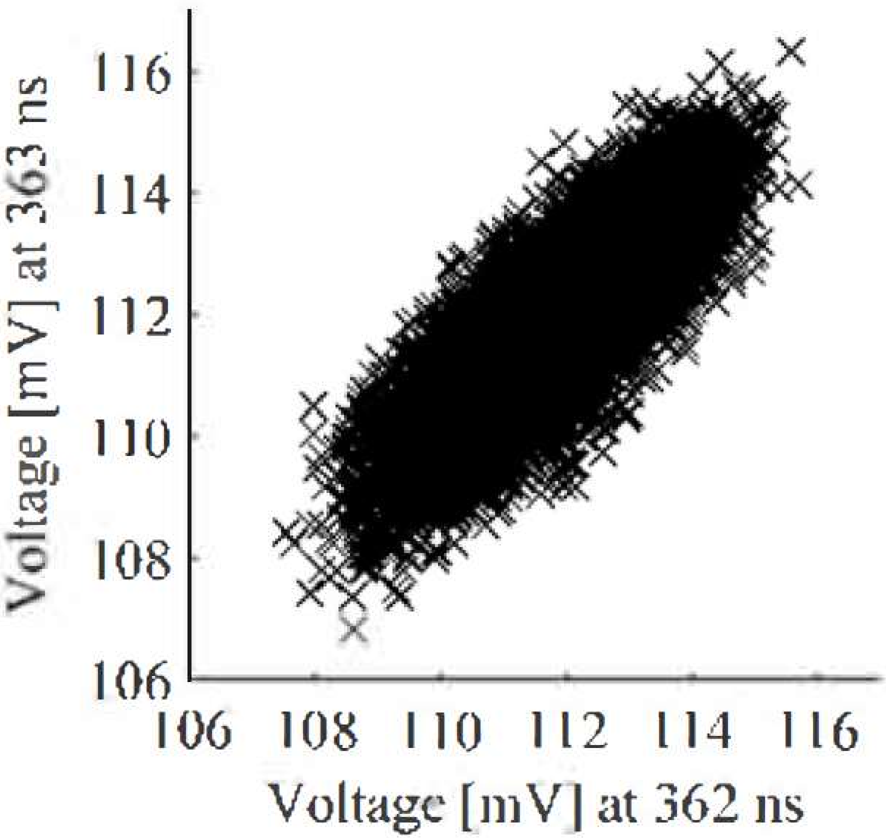

Figure 4.9. Scatter Plot: The power consumption at 362 ns is correlated to the power consumption at 363 ns.

***r* = 0.82**

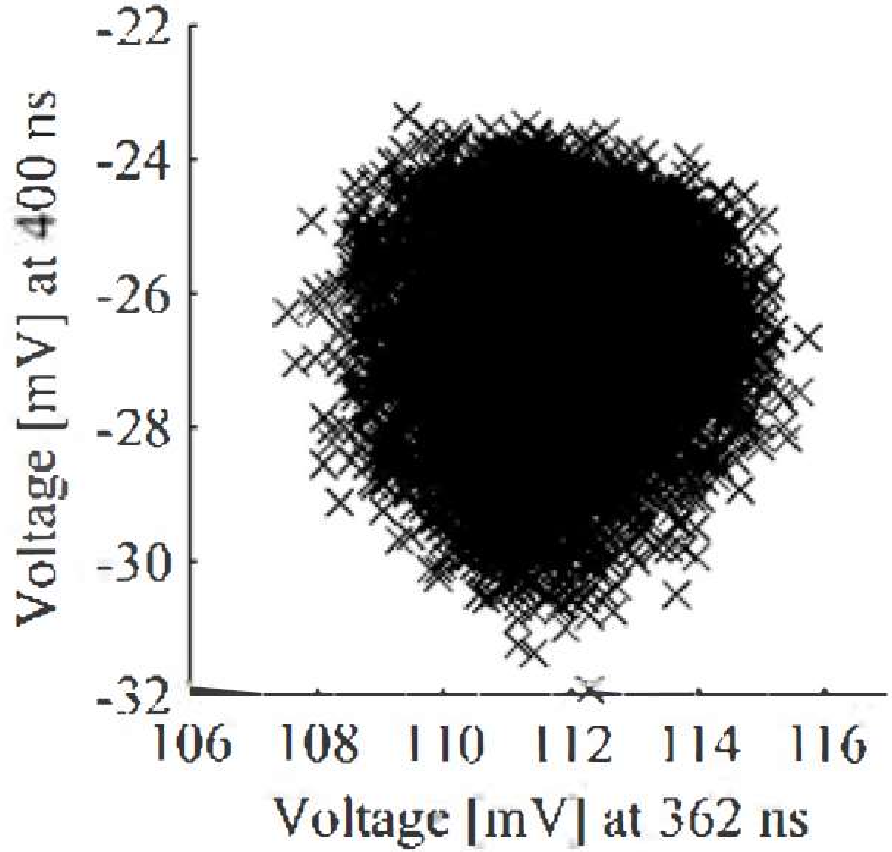

Figure 4.10. Scatter Plot: The power consumption at 362 ns is largely uncorrelated to the power consumption at 400 ns.

***r* = 0.12**