Power Analysis Part IV

Cryptographic Hardware for Embedded Systems

ECE 3170

Fall 2026

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

©Georgia Institute of Technology, 2018-2026

Reading

- This rest of this lecture covers a portion of Differential Power Analysis as explained in Chapter 1 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.

©Georgia Institute of Technology, 2018-2026

AES Power Trace

- Flat first 0.35 ms
- After receiving plaintext input at 0.35 ms, nine AES rounds occur
  - Each round appears to take 0.4 ms
- Final AES round (round 10) omits MixColumns
- At approximately 4.1 ms the microcontroller waits again
- 10 MHz ⇒ 0.1 µs (100ns) per instr ⇒ 1000 instructions in 0.1ms

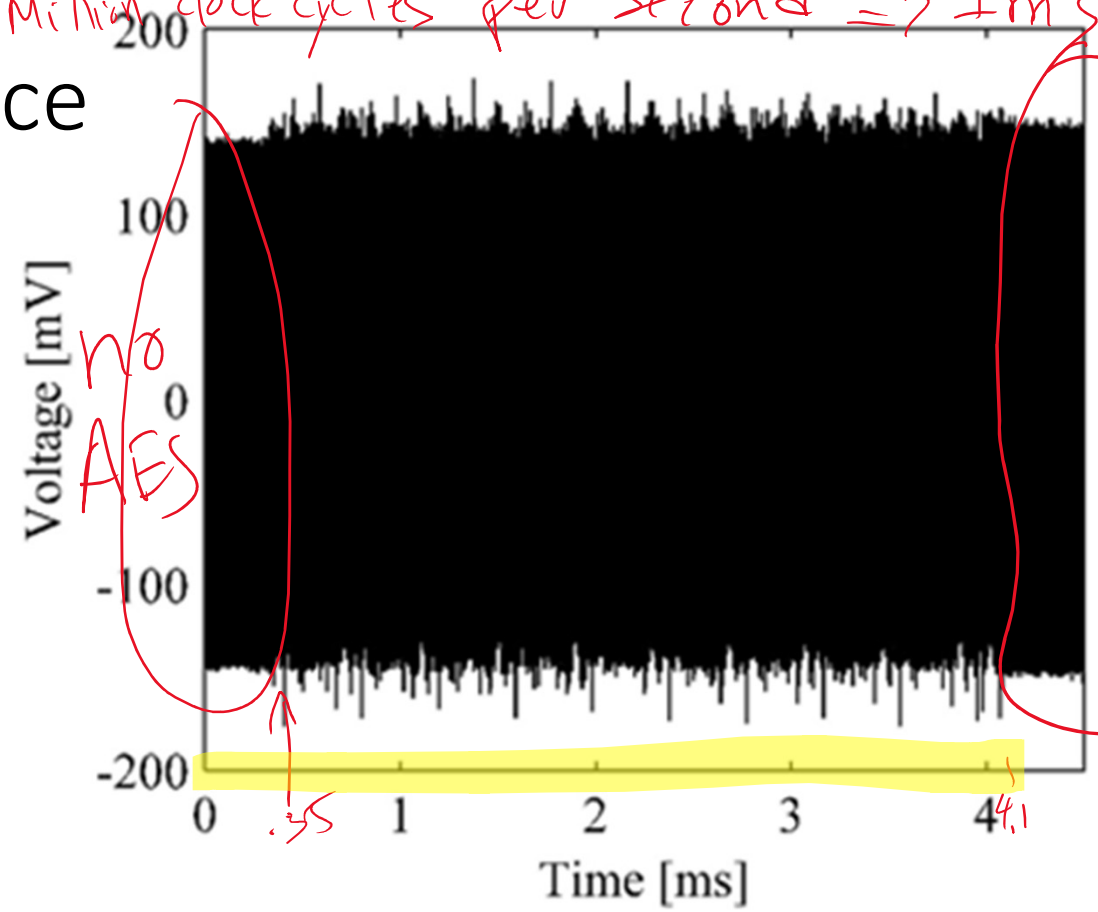


Figure 1.1. The voltage drop (power consumption) of the microcontroller while it performs an AES encryption.

Difference of Mean Power

- Consider MSB of plaintext 1st byte
  - d = most sig. bit
- Measure 1000 traces: ½ with d=1, ½ with d=0
- Calculate difference of means
- Peaks indicate dependence on value of d

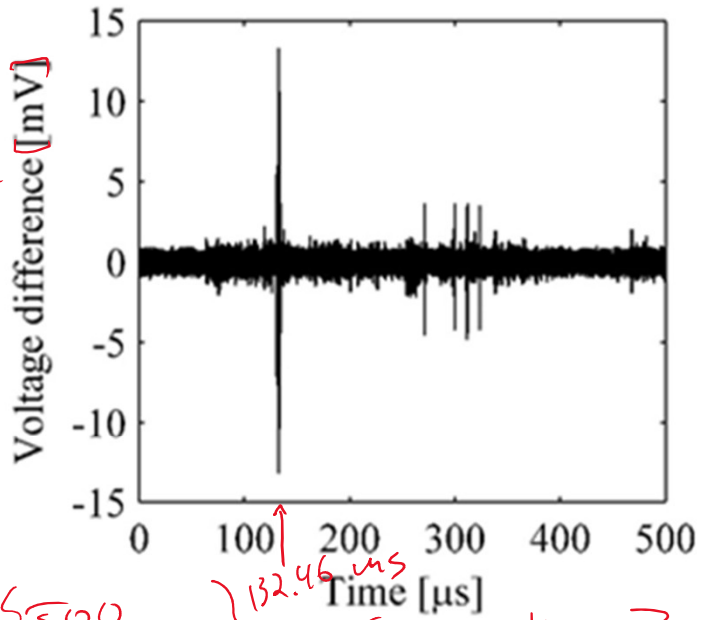


Figure 1.3. Difference of the mean power trace for $d = 1$ and the mean power trace for $d = 0$.

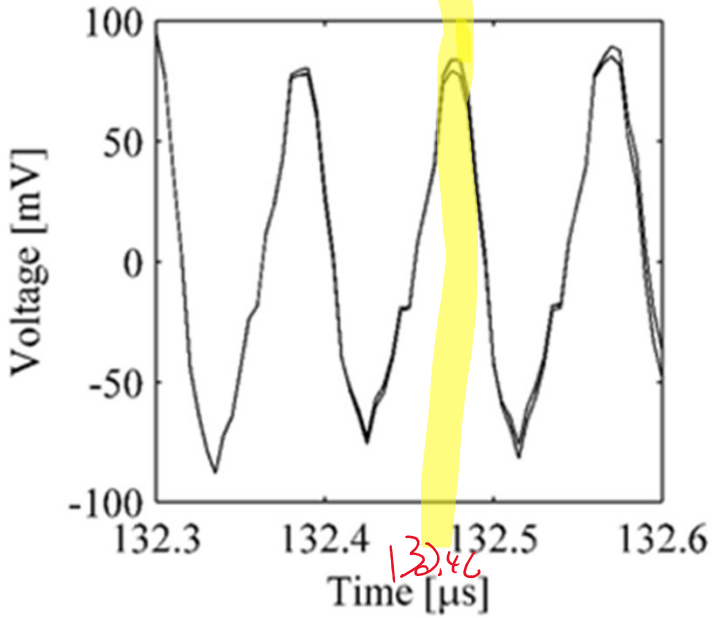


Figure 1.4. Zoomed view of the mean power trace for $d = 1$ and the mean power trace for $d = 0$.

©Georgia Institute of Technology, 2018-2026

Instruction Dependence on bit *d*

- AES S-box operation *S()* "SubBytes"
- Let *p* = first plaintext bye, *k* = first key byte
- Fig. 1.4 shows mean power traces for calc. *S(p ⊕ k)*

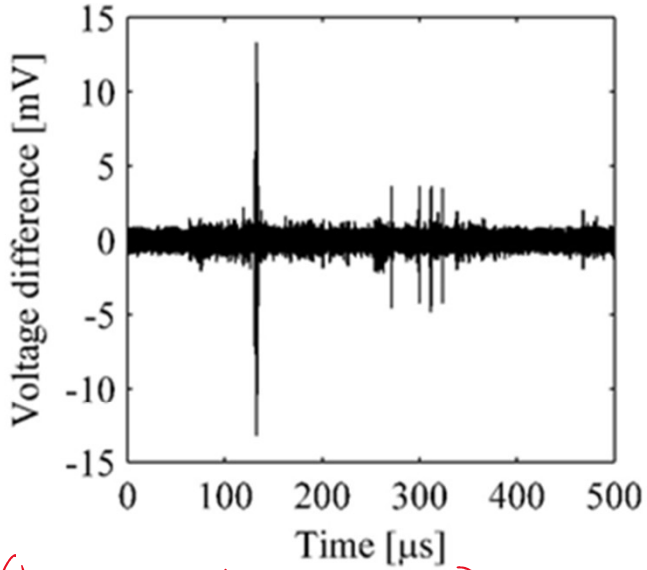


Figure 1.3. Difference of the mean power trace for $d = 1$ and the mean power trace for $d = 0$.

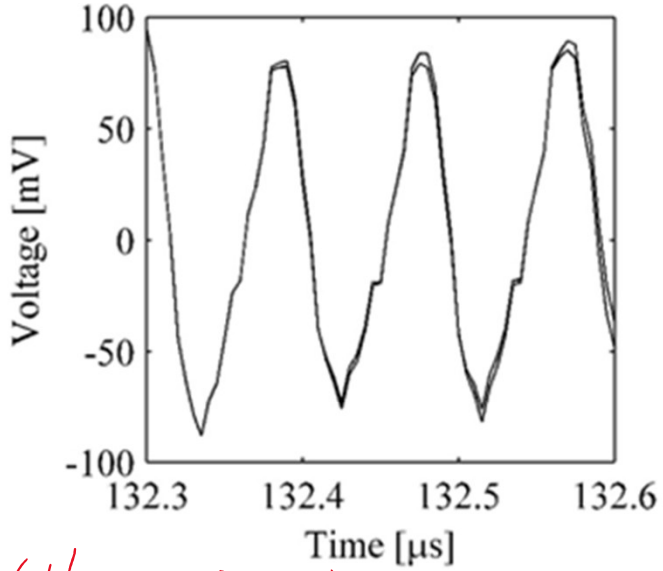


Figure 1.4. Zoomed view of the mean power trace for $d = 1$ and the mean power trace for $d = 0$.

S(b <7 bits same>) vs. S(b' <7 bits same>)

©Georgia Institute of Technology, 2018-2026

Steps in Differential Power Analysis

1. Choose an intermediate part of the algorithm to attack
   a. For example, function *f(d,k)* where *d* is a data input and *k* is a small part of the secret key stored in the device under attack
   b. Typically *d* is either plaintext or ciphertext
2. Make a large number of power measurements
3. Calculate hypothetical intermediate values
4. Map hypothetical intermediate values to resulting predicted power values
5. Compare predicted power values with the actual trace values

©Georgia Institute of Technology, 2018-2026

Difference of Mean Power

- Consider MSB v of $S(p \oplus k)$
  - v=1 vs. v=0
- Calc. difference of 1000 traces: ½ with v=1, ½ with v=0
- Note key byte k has 256 guesses
- Peaks indicate correct guess!

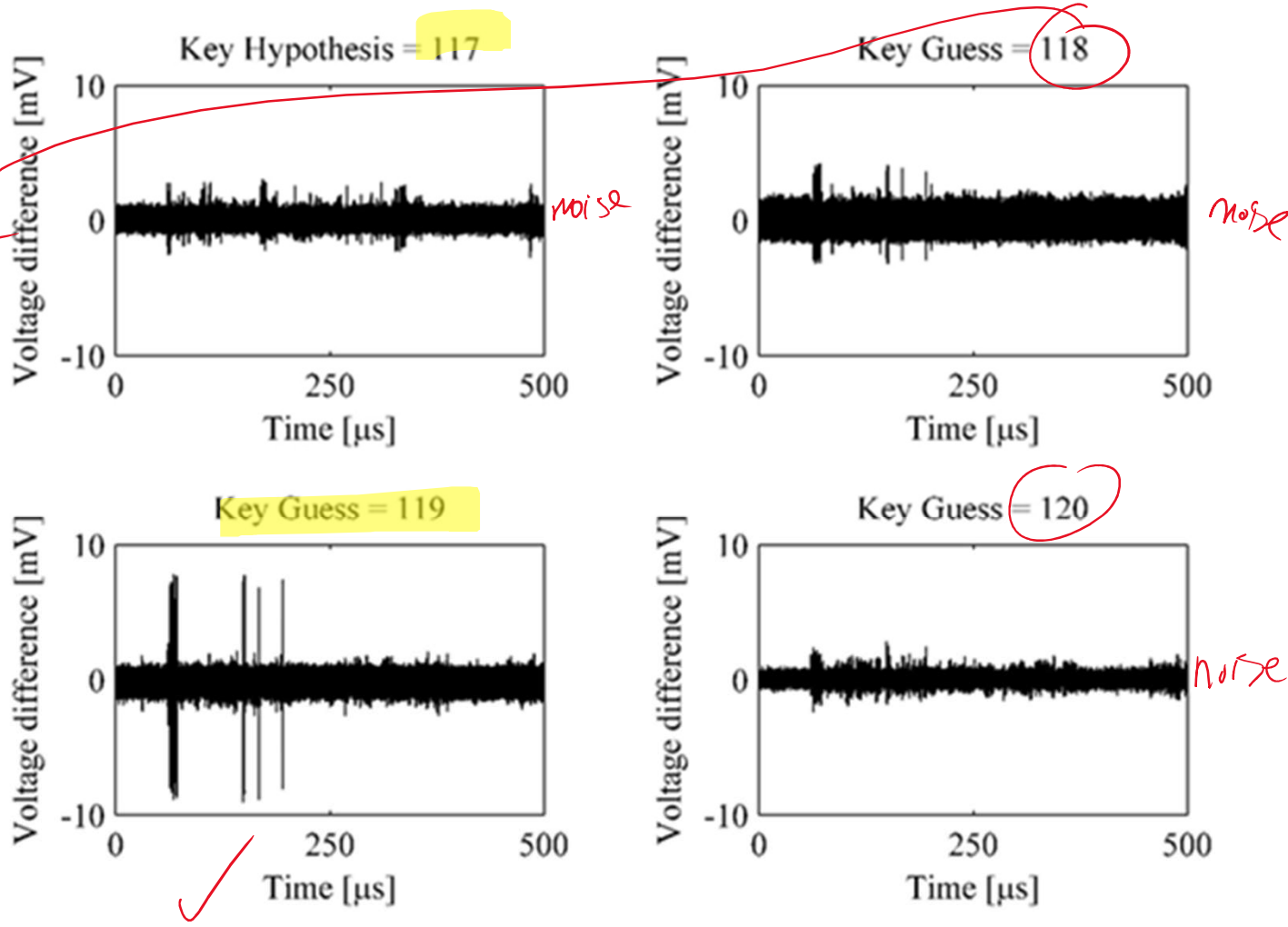


Figure 1.5. Difference plots for the key guesses 117, 118, 119, and 120.

©Georgia Institute of Technology, 2018-2026

1000 plaintext measurements

1000 power traces

$t_1, t_{50}, t_{73}, t_{99}$

if $k=9$ then MSB of $t_1 + t_{73}$ is 1 → $v=1$ $\{t_1, t_{73}\}$

$=0x09$

MSB of $t_{50} + t_{99}$ is 0 → $v=0$ $\{t_{50}, t_{99}\}$

if $k=181$ then MSB of $t_{50} + t_{73}$ is 1 → $v=1$ $\{t_{50}, t_{73}\}$

MSB of t_1, t_{99} is ϕ → $v=0$ $\{t_1, t_{99}\}$

©Georgia Institute of Technology, 2018-2026