Power Analysis Part V: DPA Cont'd

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 lecture covers a portion of Differential Power Analysis as explained in Chapter 6 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

Questions Answered by This Lecture

- How can one carry out DPA on a microcontroller running AES with the goal of finding the key?
  - Assumption # 1: the attacker can input any plaintext desired and obtain the corresponding ciphertext from the device running AES
  - Assumption # 2: the attacker can accurately measure power (either through physical access or remote access to the power trace data measurement)

©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
   a. Keep track of the known data values d_i as recording the measurements
   b. For each d_i there exists a power trace of size *T*: $\mathbf{t'}_i = (t_{i,1}, \ldots, t_{i,T})$
3. Calculate hypothetical intermediate values
   a. For each k_j (subkey), the K possible choices are $\mathbf{k} = (k_1, \ldots, k_K)$
   b. The possible choices are used in conjunction with *f(d,k)*
4. Map hypothetical intermediate values to resulting predicted power values
5. Compare predicted power values with the actual trace values

Controlling for key

©Georgia Institute of Technology, 2018-2026

Fig. 6.1 from PAA textbook

I break this fig. up into pieces to explain

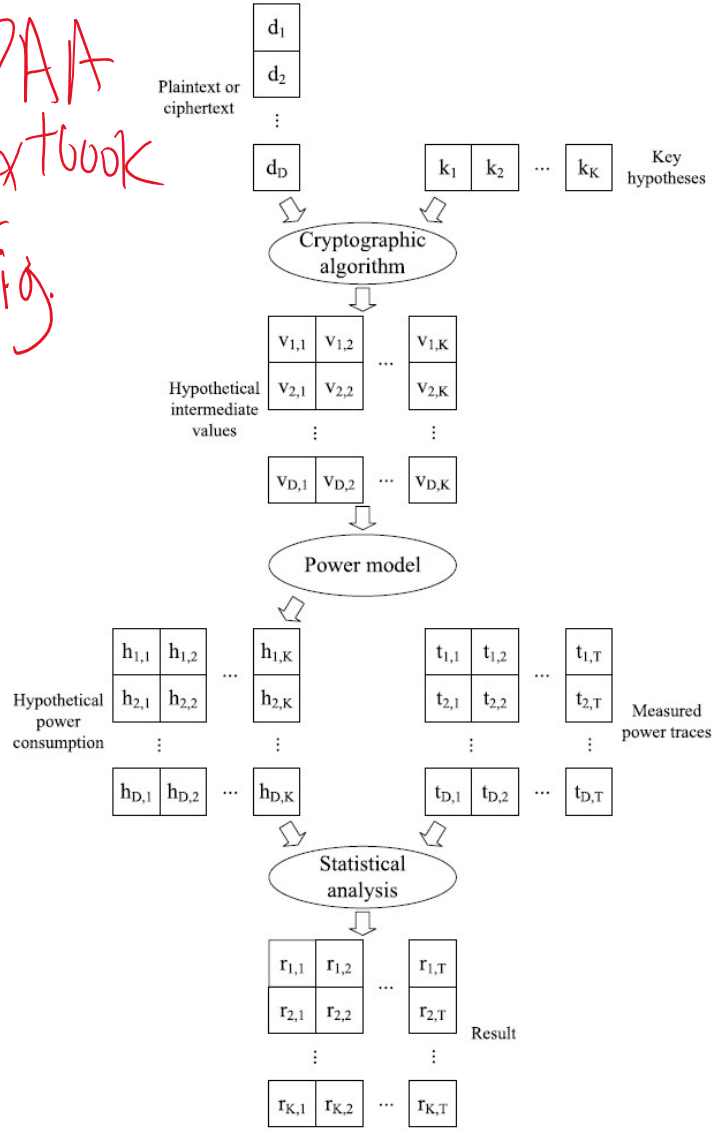
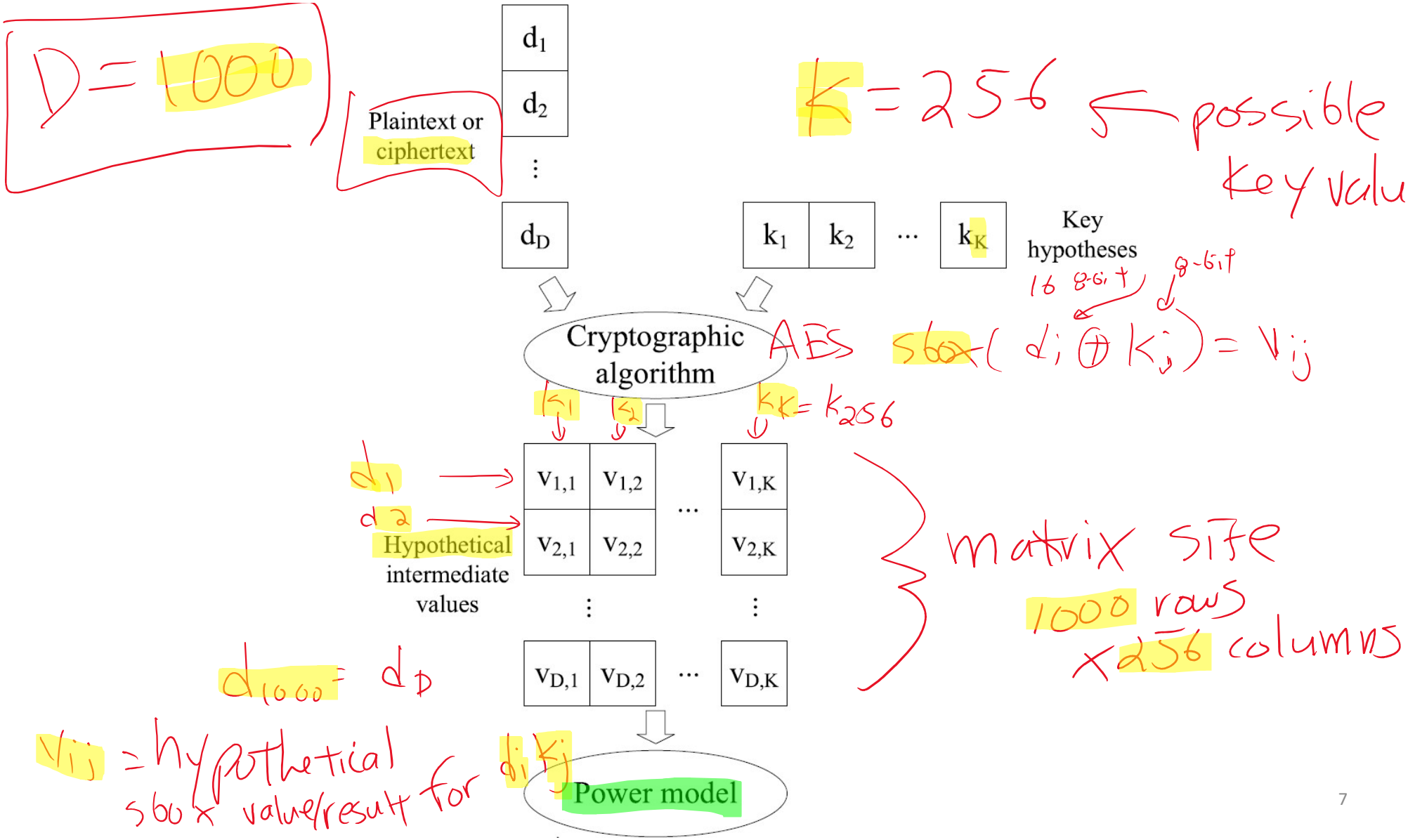


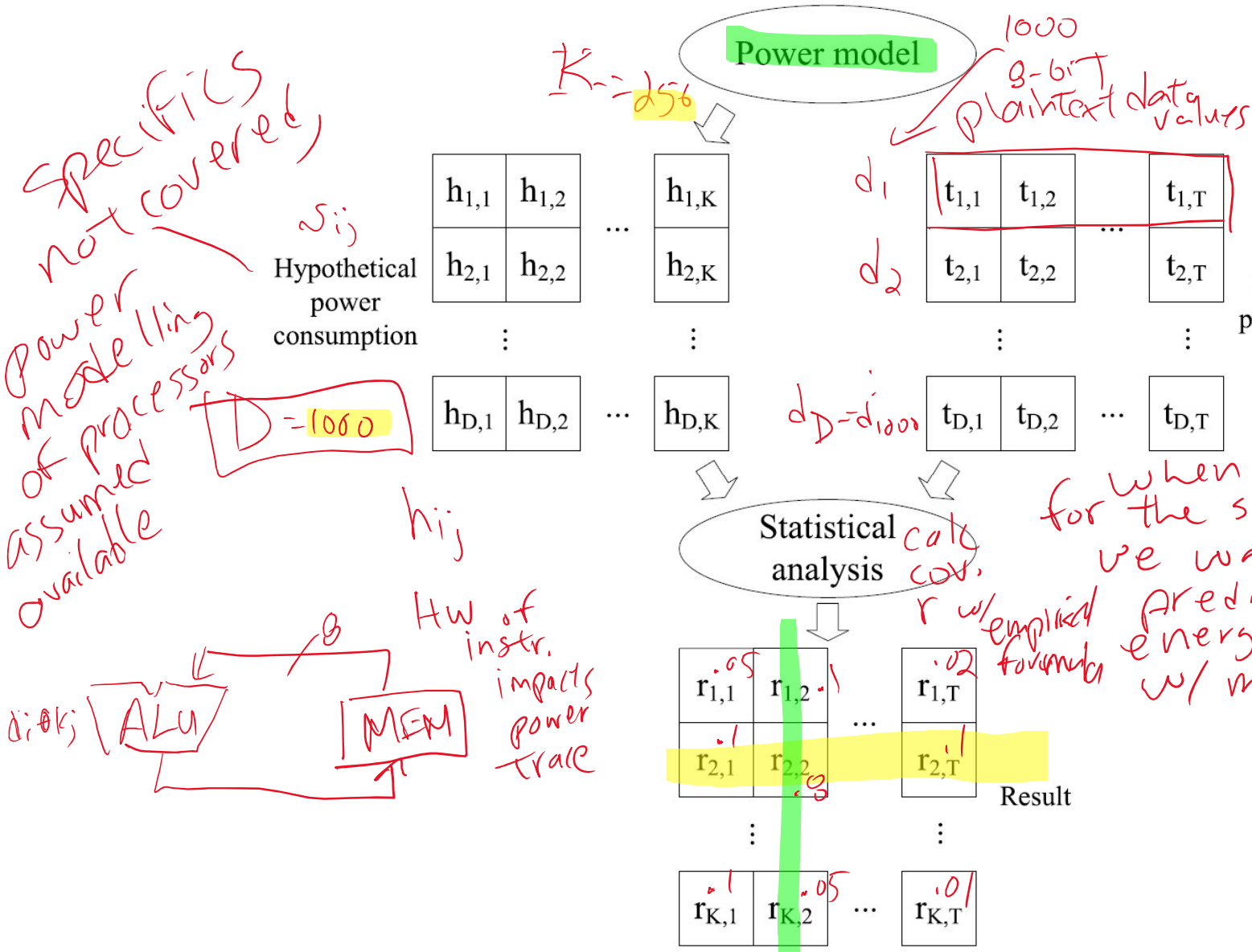
Figure 6.1. Block diagram illustrating the steps 3 to 5 of a DPA attack.

Microcontroller Example

- AES software SBOX calculation
  - s = S(*p* XOR *k*) where *p* is the plaintext and *k* is the subkey (each of size 8 bits)
- Calculate 1000 power traces
  - Each power trace corresponds to a specific plaintext input
    - Hence, there are 1000 power measurements taken for each value of the 128 bit plaintext
      - Note that the overall plaintext input size is 128 for AES, hence there are 2^{128} possible values of the overall plaintext
    - E.g., for a timeframe of 100 µs, there is a measurement for every 100 ns (10 MHz sample rate of the power measurement device, e.g., an oscilloscope)
  - A total of 1,000,000 measurements are stored in this example, e.g., from an oscilloscope based power measurement setup
    - If each measurement requires 32 bits (a word), then the filesize is 4 MB (Megabytes)

©Georgia Institute of Technology, 2018-2026


D = 1000
Plaintext or ciphertext
d1
d2
dD
k1
k2
kK
Key hypotheses
K = 256 ← possible key values
16 8-bit
8-bit
Cryptographic algorithm
AES
sbox(di ⊕ kj) = vij
k1
k2
kK = k256
d1
d2
Hypothetical intermediate values
v1,1
v1,2
v1,K
v2,1
v2,2
v2,K
vD,1
vD,2
vD,K
matrix size
1000 raws
x256 columns
d1000 = dD
vij = hypothetical sbox value/result for di kj
Power model



specifics not covered

power modelling of processors assumed available

$h_{i,j}$

HW of instr. impacts power trace

calc cov. r w/ empirical formula

T = 1000 power samples using oscilloscope

array size: 1000×1000 = 1 million

for when the MOV instruction for the sbox actually executes, we want to compare predicted/hypothetical energy consumption w/ measured

clock jitter interrupt handling

Microcontroller Example Continued

- AES software SBOX calculation
  - Let us consider the first byte (8 bits) of the overall plaintext input (128 bits)
  - s = S(*p* XOR *k*) where *p* is the plaintext and *k* is the subkey (each of size 8 bits)
- Recall we have 1000 power traces, each with a known specific value of *p*

©Georgia Institute of Technology, 2018-2026

Steps in Differential Power Analysis

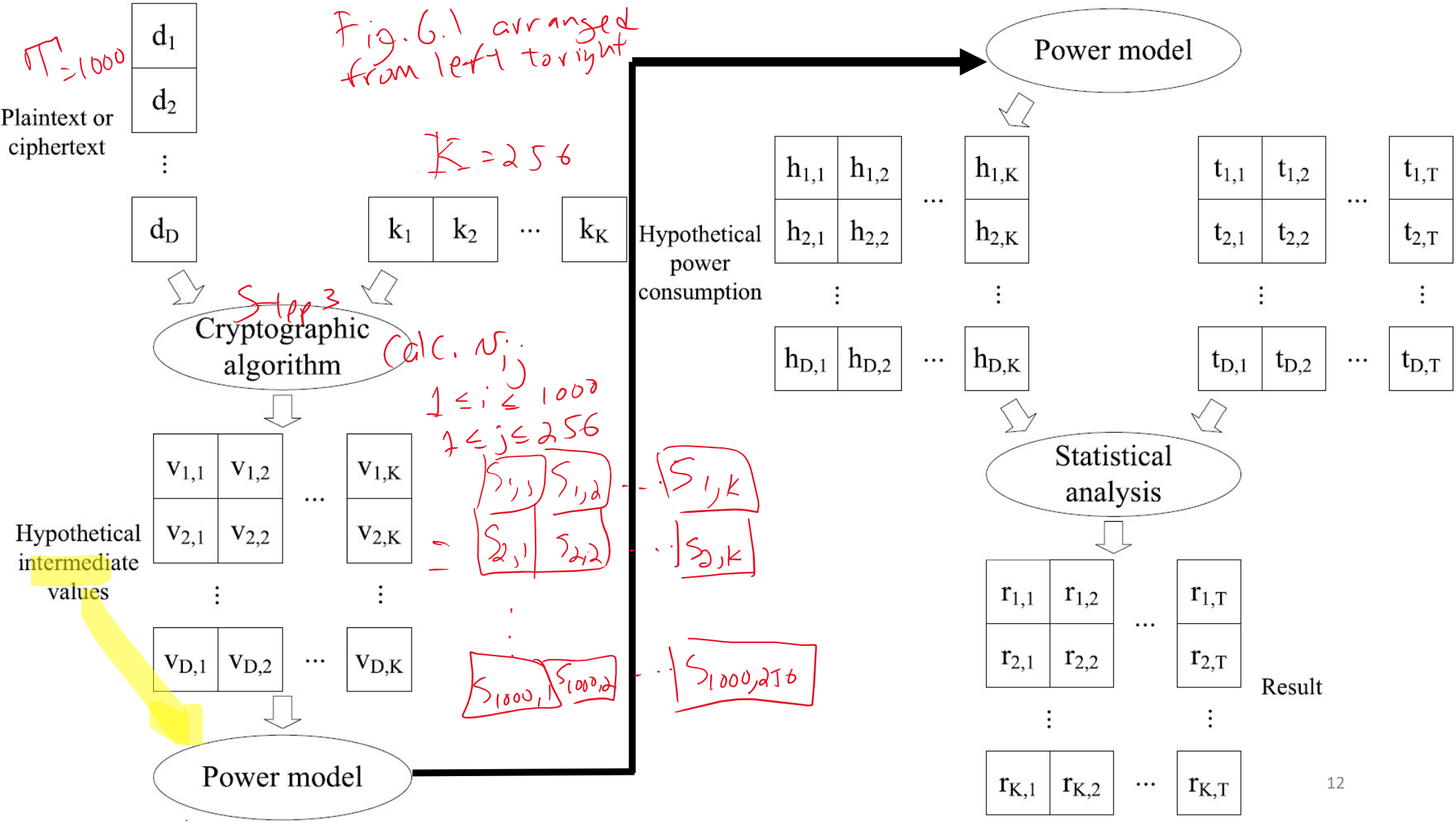
1. Choose an intermediate part of the algorithm to attack
   a. For example, function *f(d,k)* where *d* is a data input and *k* is a small part of the secret key stored in the device under attack
   b. Typically *d* is either plaintext or ciphertext
2. Make a large number of power measurements
   a. Keep track of the known data values d_i as recording the measurements
   b. For each d_i there exists a power trace of size *T*: $\mathbf{t'}_i = (t_{i,1}, \ldots, t_{i,T})$
3. Calculate hypothetical intermediate values
   a. For each *k*, the K possible choices are $\mathbf{k} = (k_1, \ldots, k_K)$
   b. The possible choices are used in conjunction with *f(d,k)*
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

Microcontroller Example Continued

- AES software SBOX calculation
  - Let us consider the first byte (8 bits) of the overall plaintext input (128 bits)
  - s = S(*p* XOR *k*) where *p* is the plaintext and *k* is the subkey (each of size 8 bits)
- Recall we have 1000 power traces, each with a known specific value of *p*
- Step 3 is to calculate hypothesized intermediate values of s = S(*p* XOR *k*)
  - Let $v_{i,j} = s_{i,j} = S(p_i \text{ XOR } k_j)$ where *i* ranges from 1 to 1000 and *j* from 0 to 256
  - Matrix **V** = $\{v_{i,j}\}$ has size 1000 rows by 256 columns

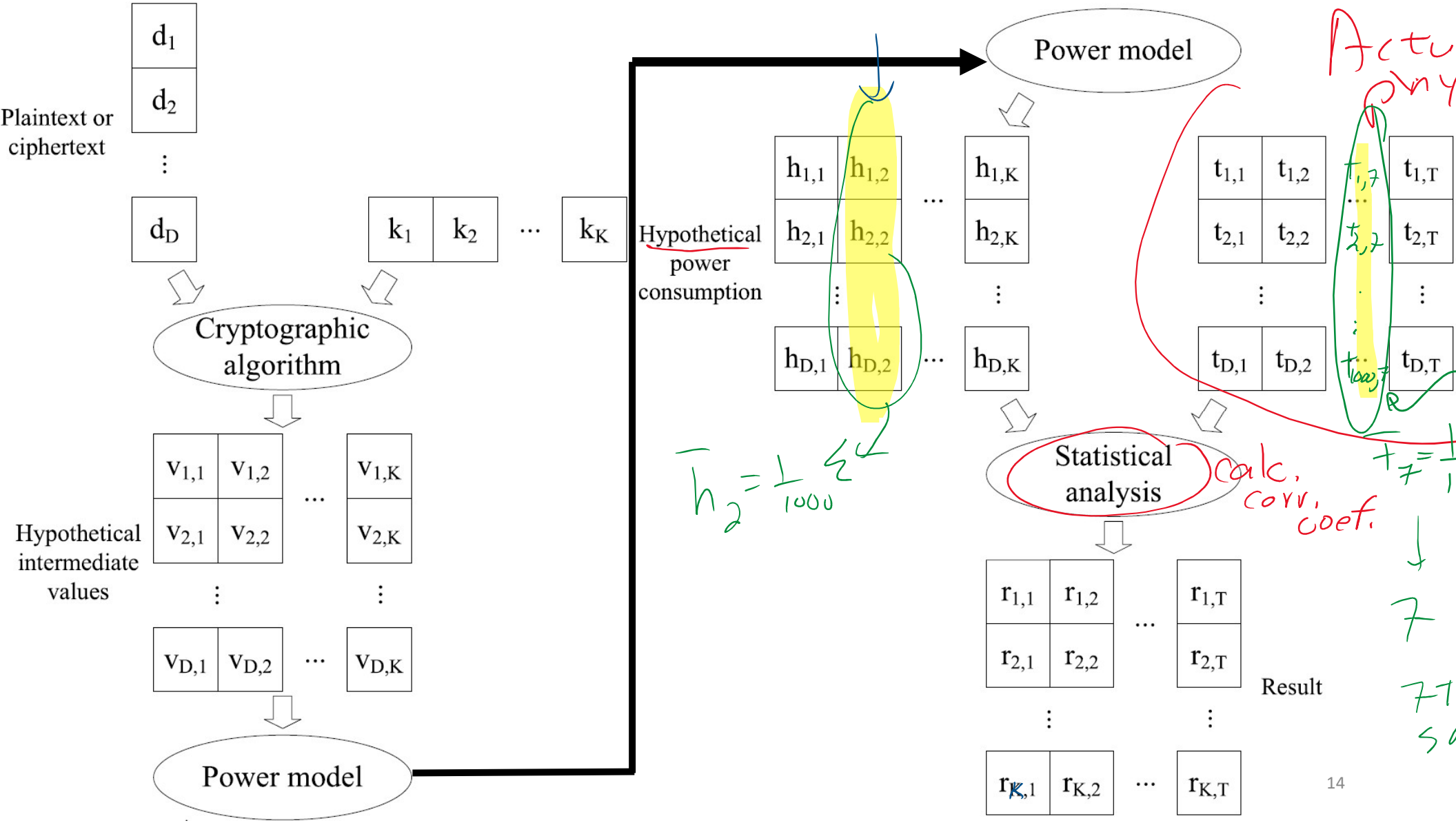
©Georgia Institute of Technology, 2018-2026


Plaintext or ciphertext
d_1
d_2
d_D
k_1 k_2 ... k_K
Cryptographic algorithm
Hypothetical intermediate values
$v_{1,1}$ $v_{1,2}$ ... $v_{1,K}$
$v_{2,1}$ $v_{2,2}$ ... $v_{2,K}$
$v_{D,1}$ $v_{D,2}$ ... $v_{D,K}$
Power model
Hypothetical power consumption
$h_{1,1}$ $h_{1,2}$ ... $h_{1,K}$
$h_{2,1}$ $h_{2,2}$ ... $h_{2,K}$
$h_{D,1}$ $h_{D,2}$ ... $h_{D,K}$
Power model
$t_{1,1}$ $t_{1,2}$ ... $t_{1,T}$
$t_{2,1}$ $t_{2,2}$ ... $t_{2,T}$
$t_{D,1}$ $t_{D,2}$ ... $t_{D,T}$
Statistical analysis
$r_{1,1}$ $r_{1,2}$ ... $r_{1,T}$
$r_{2,1}$ $r_{2,2}$ ... $r_{2,T}$
$r_{K,1}$ $r_{K,2}$ ... $r_{K,T}$
Result

Microcontroller Example Continued Again

- AES software SBOX calculation s = S(p XOR k)
- We have 1000 power traces each with a known specific value of p
- Step 3 is has calculated hypothesized intermediate values
  - **V** = $\{v_{i,j}\}$ = $\{s_{i,j}\}$ = { S(p_i XOR k_j) } of size 1000 rows by 256 columns
- Step 4 in this example maps **V** to **H**
  - Use $h_{i,j} = LSB(v_{i,j}) = LSB(s_{i,j}) = LSB(\ S(p_i \text{ XOR } k_j)\ )$
  - **H** = $\{h_{i,j}\}$ = results of an energy consumption model = an estimated set of power measurements based on a power model and assumed key values = a matrix of size 1000 rows by 256 columns

©Georgia Institute of Technology, 2018-2026


Plaintext or ciphertext
d_1
d_2
d_D
k_1 k_2 ... k_K
Cryptographic algorithm
Hypothetical intermediate values
$v_{1,1}$ $v_{1,2}$ ... $v_{1,K}$
$v_{2,1}$ $v_{2,2}$ ... $v_{2,K}$
$v_{D,1}$ $v_{D,2}$ ... $v_{D,K}$
Power model
Hypothetical power consumption
$h_{1,1}$ $h_{1,2}$ ... $h_{1,K}$
$h_{2,1}$ $h_{2,2}$ ... $h_{2,K}$
$h_{D,1}$ $h_{D,2}$ ... $h_{D,K}$
Power model
$t_{1,1}$ $t_{1,2}$ ... $t_{1,T}$
$t_{2,1}$ $t_{2,2}$ ... $t_{2,T}$
$t_{D,1}$ $t_{D,2}$ ... $t_{D,T}$
Statistical analysis
$r_{1,1}$ $r_{1,2}$ ... $r_{1,T}$
$r_{2,1}$ $r_{2,2}$ ... $r_{2,T}$
$r_{K,1}$ $r_{K,2}$ ... $r_{K,T}$
Result

Microcontroller Example Continued Again

- AES software SBOX calculation s = S(*p* XOR *k*)
- We have 1000 power traces each with a known specific value of *p*
- Step 3 is has calculated hypothesized intermediate values
  - **V** = $\{v_{i,j}\} = \{s_{i,j}\} = \{ S(p_j \text{ XOR } k_j) \}$ of size 1000 rows by 256 columns
- Step 4 in this example maps **V** to **H**
  - Use $h_{i,j} = LSB(v_{i,j}) = LSB(s_{i,j}) = LSB(S(p_j \text{ XOR } k_j))$
  - **H** = $\{h_{i,j}\}$ = results of an energy consumption model = an estimated set of power measurements based on a power model and assumed key values = a vector of size 1000 rows by 256 columns
- Step 5 is to calculate the covariance of **H** with the actual trace data

©Georgia Institute of Technology, 2018-2026

Recall we estimate $\mu = E(X)$ with the average $\bar{X}$

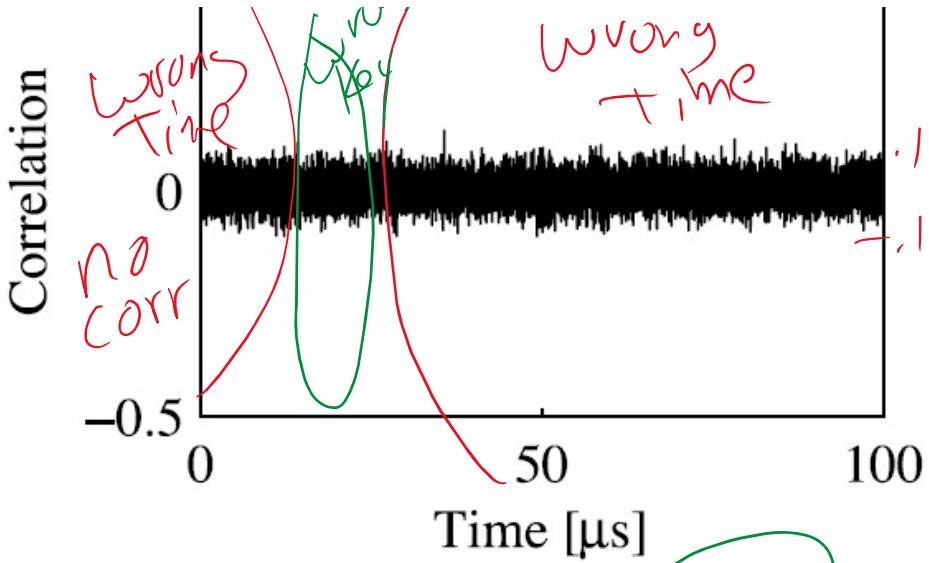
Calculated empirically: $\bar{x} = \frac{1}{1000} \sum_{i=1}^{1000} x_i$

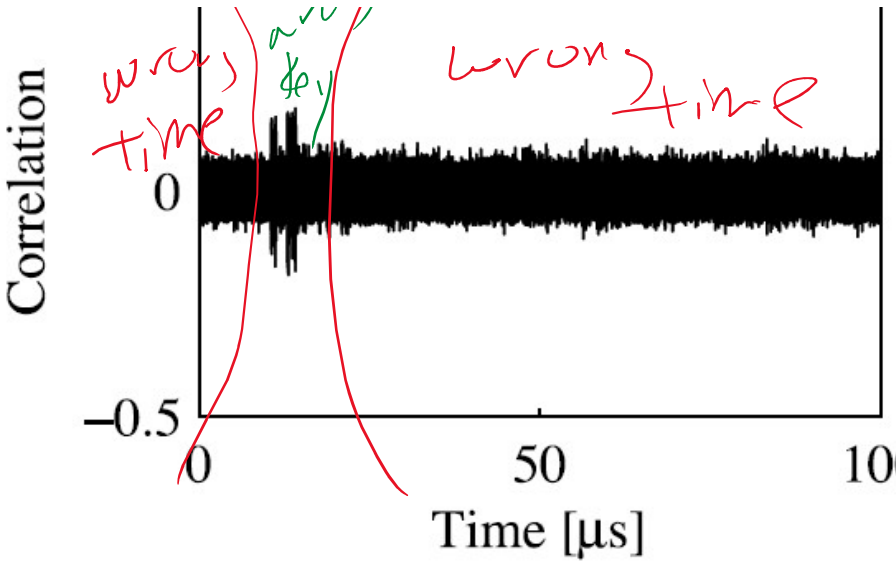
for example, 2nd row, $\bar{h}_2 = \frac{1}{1000} \sum_{i=1}^{1000} h_{i,2}$ $\quad j = 7$ $\quad \bar{t}_7 = \frac{1}{1000} \sum_{i=1}^{1000} t_{i,7}$

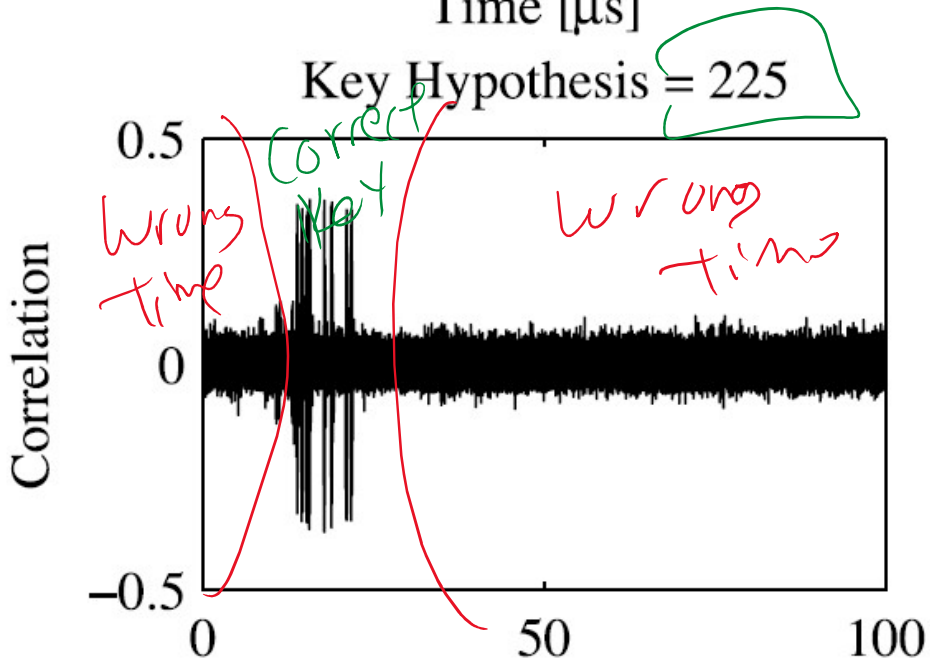
$$r_{i,j} = \frac{\sum_{d=1}^{D} (h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D} (h_{d,i} - \bar{h}_i)^2 \cdot \sum_{d=1}^{D} (t_{d,j} - \bar{t}_j)^2}} \qquad (6.2)$$

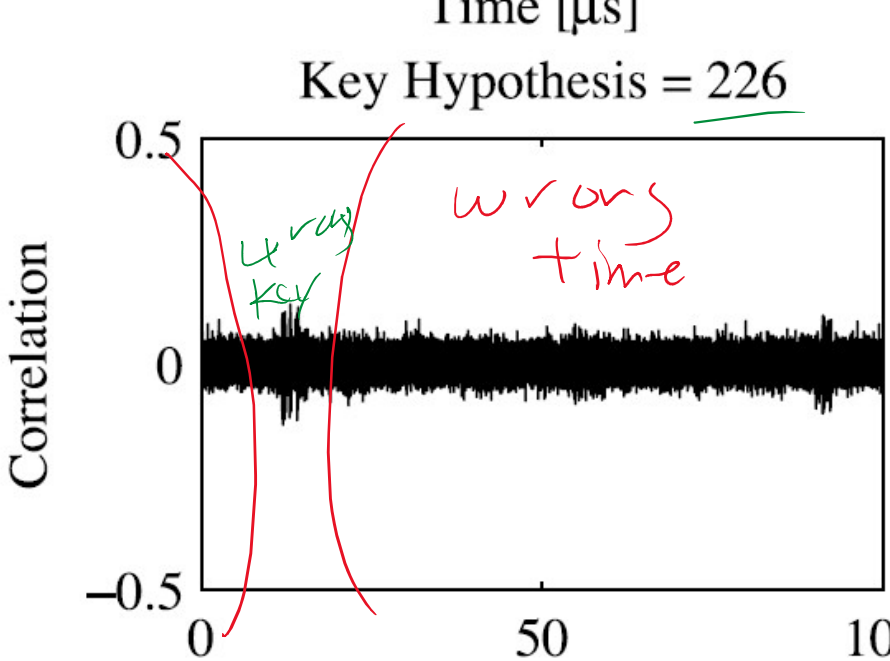
$$r_{2,7} = \frac{\sum_{d=1}^{1000} (h_{d,2} - \bar{h}_2)(t_{d,7} - \bar{t}_7)}{\sqrt{\left(\sum_{d=1}^{1000} (h_{d,2} - \bar{h}_2)^2\right)\left(\sum_{d=1}^{1000} (t_{d,7} - \bar{t}_7)^2\right)}}$$

©Georgia Institute of Technology, 2018-2026


Correlation
0.5
0
−0.5
0
50
100
Time [µs]


Correlation
0
−0.5
0
50
Time [µs]


Key Hypothesis = 225
Correlation
0.5
0
−0.5
0
50
100


Key Hypothesis = 226
Correlation
0.5
0
−0.5
0
50

Comments

p_i = plaintext input i

h_{ij}
$1 \le i \le 1000$
$1 \le j \le 256$
j corresponds to a key value

T_{ij}
$1 \le i \le 1000$
$1 \le j \le 10000$
j corresponds to a specific trace time (no relationship to any diff. key guess)

Consider column j from $[h_{ij}]$

e.g., $j = 2$

$\overline{h_2} = \sum_{i=1}^{D=1000} h_{i,2}$

There are 256 ways to divide up $t_{i,3}$
e.g., based on MSb = 1 vs. 0
consider col. 7 from $[T_{ij}]$:

$\overline{T_7} = \sum_{i=1}^{D} t_{i,7}$

r_{kl} compares column k from $[h_{ij}]$ to column l of $[T_{ij}]$

result: $[r_{ij}]$ e.g., $r_{27} = \frac{\sum \cdots}{\sqrt{\sum 2 \left(\sum 2\right)}}$

©Georgia Institute of Technology, 2018-2026

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., $-1 \le \rho \le 1$ and also thus $-1 \le r \le 1$

©Georgia Institute of Technology, 2018-2026

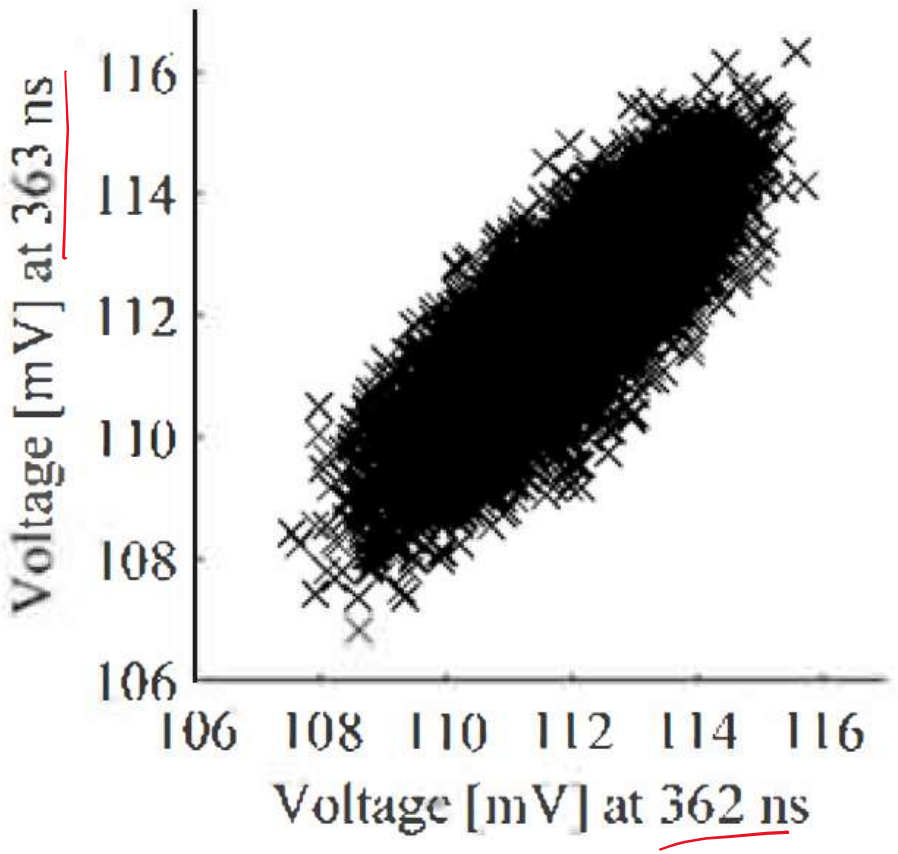


Figure 4.9. Scatter Plot: The power consumption at 362 ns is correlated to the power consumption at 363 ns.

$r = 0.82$

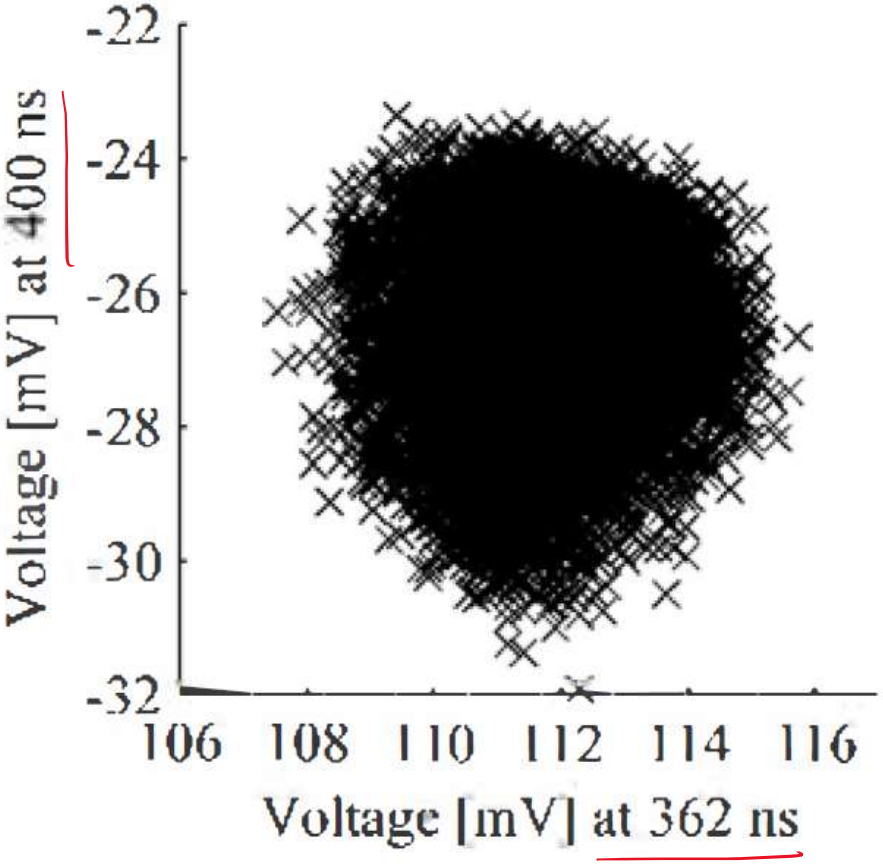


Figure 4.10. Scatter Plot: The power consumption at 362 ns is largely uncorrelated to the power consumption at 400 ns.

$r = 0.12$

©Georgia Institute of Technology, 2018-2026