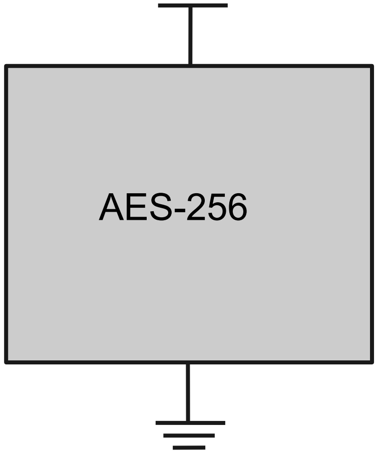
# Side Channel Attacks

## Differential Power Analysis

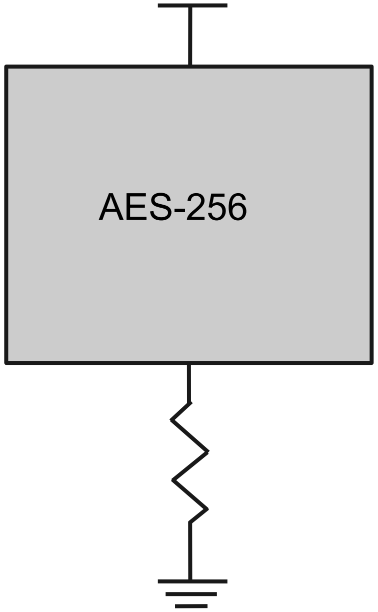
# Power Consumption

- Power consumption depends on the inputs to a circuit.
- We can reveal information about the circuit by observing the power consumption.

# Data Acquisition

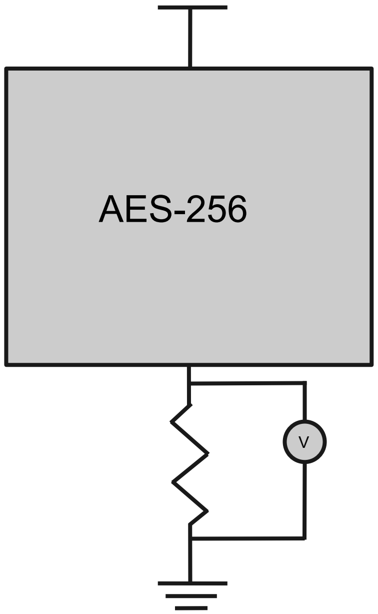


# Data Acquisition



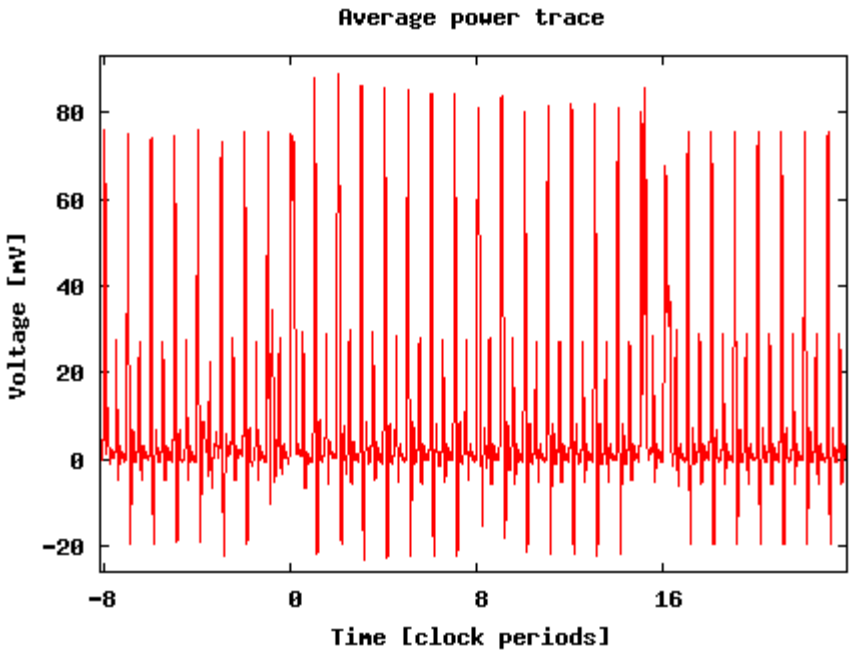

- Insert a small resistor at the ground pin.
- ~ 5 - 10 ohm

# Data Acquisition




- Insert a small resistor at the ground pin.
- ~ 5 - 10 ohm
- Use an oscilloscope to measure the voltage across the resistor

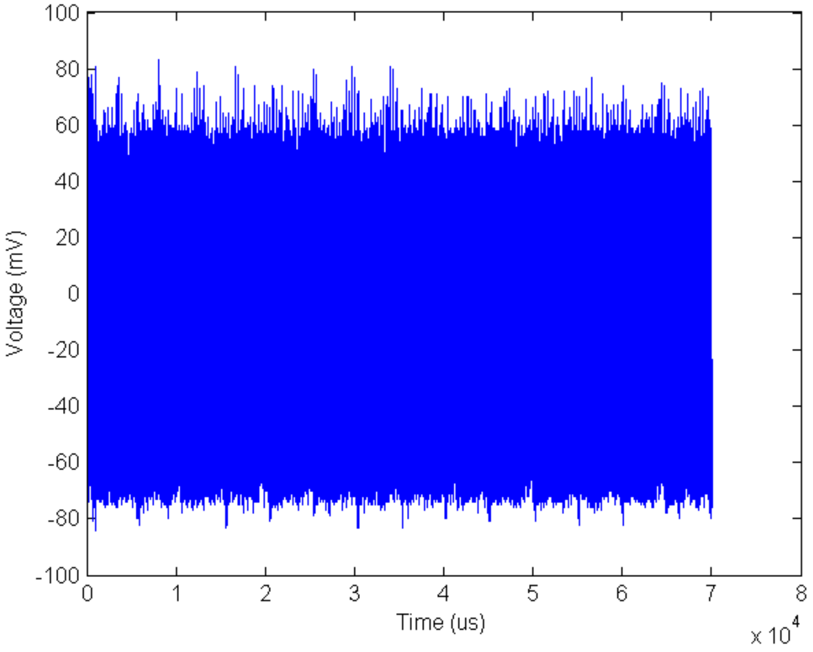
# Power Trace



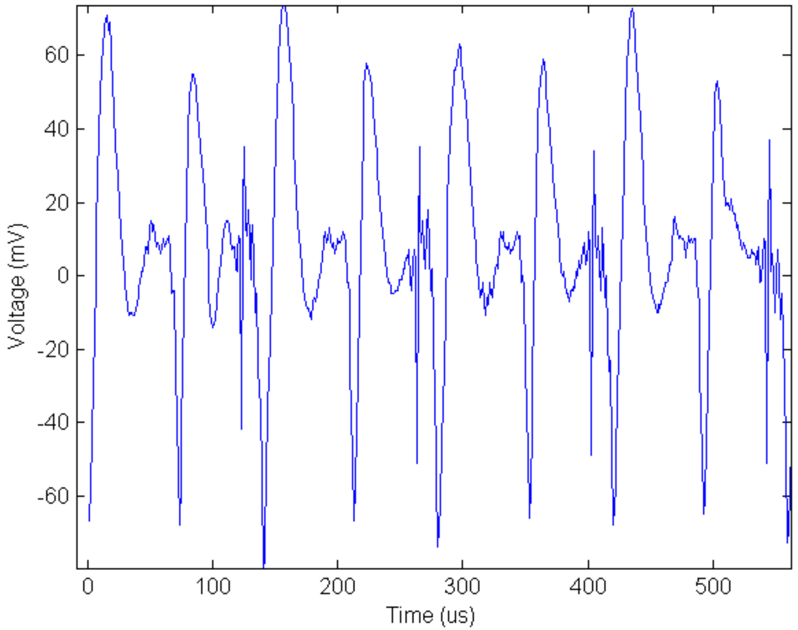

- We can see the 16 rounds of DES on this trace.
- Notice the variation in voltage between the rounds.

Source: http://www.dpacontest.org/img/secmatv1ASIC_avg.png

# Power Trace



100
80
60
40
20
0
-20
-40
-60
-80
-100
Voltage (mV)
0 1 2 3 4 5 6 7 8
Time (us)
x 10^4

60
40
20
0
-20
-40
-60
Voltage (mV)
0 100 200 300 400 500
Time (us)

# Hamming Weight Model

- Count the number of ‘1s’ in a binary number.
- Model each bit as a capacitor.
- A ‘1’ means we charge the capacitor.
- A ‘0’ means we don’t charge the capacitor.

# Hamming Weight Model

- Example:
  - 0x67 = 0110 0111
  - HW(0x67) = 5

# Hamming Distance Model

- Count the number of bits that differ in two binary numbers.
- Represents an XOR gate.
- A bit that changes uses more power than one that doesn’t change.

# Hamming Distance

- Example
  - 0x53 = 0101 0011
  - 0x78 = 0111 1000
  - XOR(0x53, 0x78) = 0010 1011
  - HD(0x53, 0x78) = 4

# DPA Example: RSM

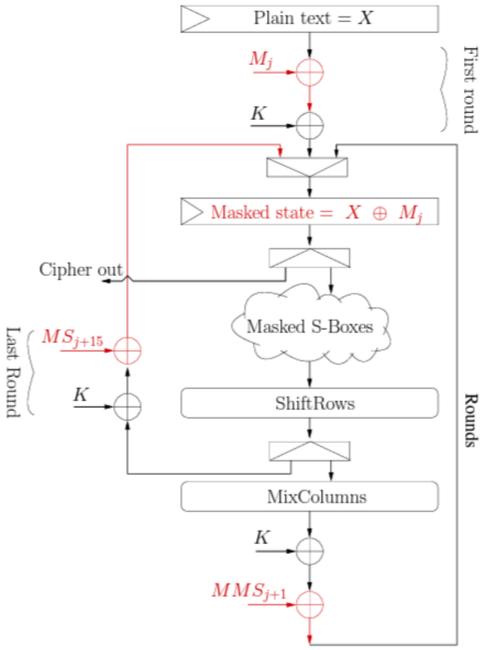



Figure 3. Linear part of the RSM datapath.

- Plaintext is masked prior to encryption.

# DPA Example: RSM

- Given:
  - M = {0x00, 0x0F, 0x36, 0x39, 0x53, 0x5C 0x65, 0x6A, 0x95, 0x9A, 0xA3, 0xAC, 0xC6, 0xC9, 0xF0, 0xFF}
  - Randomly generated offset shifts masks.
  - Offset updated after encrypting one block.

# DPA Example: RSM

- Need to determine mask offset in order to mount DPA attack.
- Target address bus when reading masks from memory.

# DPA Example: RSM

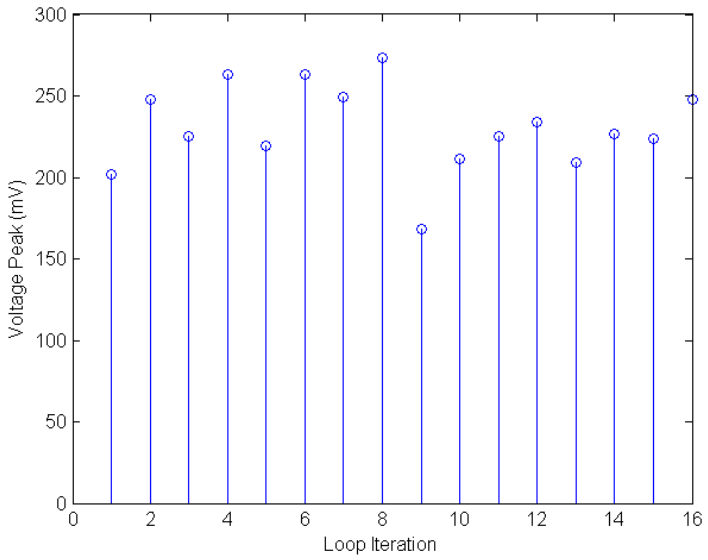
- Use hamming weight to guess power consumption of the least significant byte of the address.

- h = HD({0x0, 0x1, 0x2, 0x3, 0x4, 0x5, 0x6, 0x7, 0x8, 0x9, 0xA, 0xB, 0xC, 0xD, 0xE, 0xF})
- h = {0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4}

# DPA Example: RSM

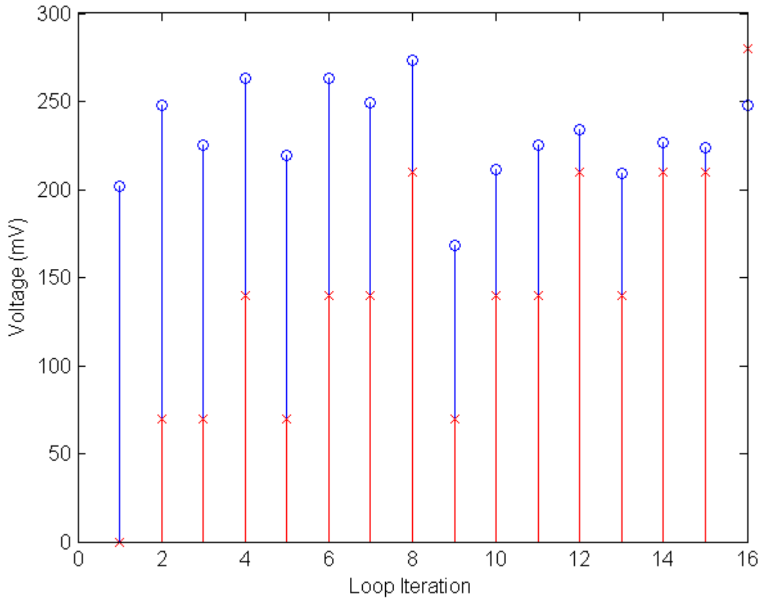
- We expect to see a pattern like one of the following:
  - h = {0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4}
  - h = {1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 0}
  - h = {1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 0, 1}
  - …
  - h = {4, 0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3}

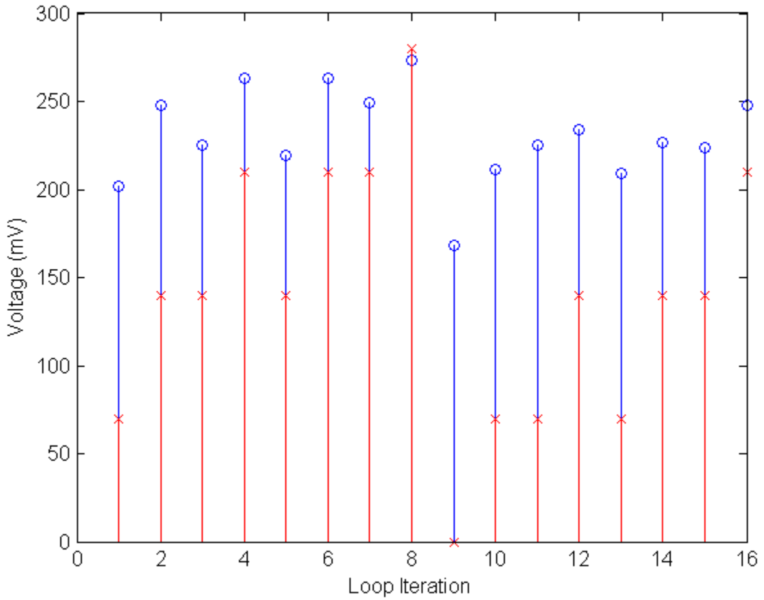
# DPA Example: RSM




- Select points of interest from power trace.
- Access memory each loop iteration.

# DPA Example: RSM



# DPA Example: RSM

- Use Pearson Correlation Coefficient to find best offset.

| Offset | Correlation | Offset | Correlation |
|---|---|---|---|
| 0x0 | .4634 | 0x8 | .9347 |
| 0x1 | -.3055 | 0x9 | .0466 |
| 0x2 | -.0181 | 0xA | .1942 |
| 0x3 | -.4194 | 0xB | -.3935 |
| 0x4 | .0386 | 0xC | .3599 |
| 0x5 | -.246 | 0xD | -.4065 |
| 0x6 | .1217 | 0xE | -.0388 |
| 0x7 | -.1709 | 0xF | -.5075 |

# DPA Example: RSM

- To recover the key:
  - Use hamming distance between key guess and masked plaintext to estimate power consumption.
  - Calculate the correlation coefficient between hypothetical power consumption and the measured power consumption.
- Requires many power traces.

# Questions?

- For more information, see:
  - www.dpacontest.org
  - http://link.springer.com/chapter/10.1007/3-540-48405-1_25#page-2