Assessing CPA Resistance of AES with Different Fault Tolerance Mechanisms

Hoda Pahlevanzadeh, Jaya Dofe, and Qiaoyan Yu
University of New Hampshire
Durham, NH, USA 03824
Email: Qiaoyan.Yu@unh.edu
Outline

• Security threats on hardware
  • Fault attack
  • Side-channel attack (SCA)
  • Combined attack

• Impact of existing countermeasures for fault attack on cryptosystem against SCA

• Factors affect the efficiency of SCA
Security Challenges in IC

- Unauthorized disclosure of information
- Unauthorized withholding of information
- Unauthorized users access

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
IC Vulnerability to an Attack

IC Vulnerability to Natural and Intentional Faults

Unified Framework for Reliability and Security of IC

Reliability
- Permanent Faults
- Intermittent Faults
- Transient Faults
- Physical Attacks
  - Side-Channel Analysis Attack
  - Fault Analysis Attack
  - Combined Attack

Security
- Hardware Trojans
- Counterfeit Chips
- Reverse Engineering
- IP Piracy
IC Security Vulnerability to Protection Circuits

Attack on AES SBox, no fault detection method.

With parity based fault detection method.

With residue code modulo 3 based fault detection method.

F. Regazzoni et al., DFT, 2008.
Side Channel Analysis Attack

SCA Countermeasures
- Randomization (Masking)

Power consumption
Time variation
Electromagnetic radiation
Thermal radiation

 Plaintext → Cryptosystem → Ciphertext

Cryptosystem
Secret Key

Graph showing data and power trace view.
Fault Analysis Attack

Laser fault injection equipment

Fault Analysis Attack

\[ \text{Plaintext} \xrightarrow{\text{Cryptosystem}} \text{Ciphertext} \]

\[-\xrightarrow{\text{Secret Key}}-\]

Clock glitch

- DMR
- Inverse function
- ECC

Combined Attack

Plaintext → Cryptosystem → Ciphertext

Power consumption

Secret Key

Correlation vs. Number of measurements

Right subkey guess

AES Cipher

Plaintext → KeyExpansion → AddRoundKey → START

KeyExpansion → SubBytes → ShiftRows → MixColumns → AddRoundKey

Nr = 9, 11 or 13

AddRoundKey → SubBytes → ShiftRows → AddRoundKey → END

Ciphertext
Impact of existing countermeasures for fault attack on cryptosystem security

Different fault detection methods

Fault detection methods on different modules
Fault Detection Methods

CPA Attack on AES

Guess the first subkey

- Store the intermediate ciphertexts
- Calculate the ciphertext

Record the power consumption

CPA Attack on AES

FD in S-Box

FD in MixColumn
### CPA Attack on AES

\[ r_{i,j} = \frac{D \sum_{d=1}^{D} h_{d,i} t_{d,j} - \sum_{d=1}^{D} h_{d,i} \sum_{d=1}^{D} t_{d,j}}{\sqrt{\left( \sum_{d=1}^{D} h_{d,i} \right)^2 - D \left( \sum_{d=1}^{D} h_{d,i}^2 \right)} \left( \sum_{d=1}^{D} t_{d,j} \right)^2 - D \left( \sum_{d=1}^{D} t_{d,j}^2 \right)}} \]

Convert the ciphertext to power trace

\[ h = aH(D) + b \]

---


<table>
<thead>
<tr>
<th>NO. of Power Trace</th>
<th>Correlation Coefficient factor</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>NO. of Power Trace</th>
<th>Correlation Coefficient factor</th>
</tr>
</thead>
</table>
Experimental Setup

Capture

Analyzer

- Parameter: Values
  - CFA Algorithm: Progressive
  - Hardware Model: Crypto Algorithm AES-128
  - Leakage Model: HD AES Last Round State

- Point Setup:
  - Starting Point: 0
  - Ending Point: 356

- Traces Settings:
  - Starting Trace: 0
  - Traces per Attack: 6000
  - Attack Runs: 1
  - Reporting Interval: 700
<table>
<thead>
<tr>
<th>Subkey NO.</th>
<th>Subkey Guess</th>
<th>Correlation coefficient factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>E6, 5B, 04, C4, ED, AD, 82, 22, ED, 36, 6D, 96, 3B</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0.063, 0.0472, 0.0937, 0.0949, 0.0661, 0.0675, 0.0531, 0.0579, 0.0542, 0.0515, 0.0663, 0.0626, 0.0823, 0.0544, 0.0541</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0.0416, 0.0425, 0.0426, 0.0428, 0.0428, 0.0428, 0.0429, 0.0430, 0.0431, 0.0432, 0.0433, 0.0434, 0.0435, 0.0436, 0.0437</td>
</tr>
</tbody>
</table>
Impact of FD on SCA Attack

FD: Parity check code

Number of Power Traces vs. Partial Guessing Entropy

- Subkey 0
- Subkey 1
- Subkey 2
- Subkey 3
- Subkey 4
- Subkey 5
- Subkey 6
- Subkey 7
- Subkey 8
- Subkey 9
- Subkey 10
- Subkey 11
- Subkey 12
- Subkey 13
- Subkey 14
- Subkey 15
Impact of Different Hardware Redundancy-Based FD Methods on SCA Attack

Existence of hardware redundancy-based FD increase the efficiency of CPA

Use information redundancy-based FD
Impact of Different Power Models in CPA Attack

Ref. ciphertext

Real ciphertext

HW: 3

Previous ciphertext

Real ciphertext

HD: 6

<table>
<thead>
<tr>
<th>Number of Power Traces</th>
<th>APGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>700</td>
<td>5000</td>
</tr>
<tr>
<td>2100</td>
<td>4900</td>
</tr>
<tr>
<td>3500</td>
<td>6300</td>
</tr>
</tbody>
</table>

Ref. ciphertext

Real ciphertext

Previous ciphertext

Real ciphertext

S-Box

Hamming Distance

Hamming Weight

1400
Impact of Different Power Models in CPA Attack

Adding Parity based FD

Number of Power Traces

Attack on AES SBox, no fault detection method.

Key distinguishable

Correlation Coefficient factor

Decreases the robustness of the cryptographic algorithm

With parity based fault detection method.

Key distinguishable

Increases the robustness of the cryptographic algorithm

Two Approaches to Study the Impact of Different FDs

Assessing the process of designing a suitable protection
Conclusion

- As the combination of FA and SCA attacks is emerging as an advanced attack, effective countermeasure for the combined attack is needed.
- One countermeasure for a particular attack can influence the other attack positively or negatively.
- Our experimental results indicate that the effective factors on CPA efficiency include
  - Type of redundancy
  - Module under protection
  - CPA attack power model
Thank you!

Any Questions?