Side Channel Attacks

Makoto Nagata
Graduate School of Science, Technology and Innovation
Kobe University
1-1 Rokkodai, Nada, Kobe, Japan
nagata@cs.kobe-u.ac.jp
Outline

▷ Physical attacks
▷ On-chip security sensor circuits
▷ Simulation technique of side-channel leakage
▷ Conclusions
Advent of Adversary among IC Chips

Crypto attacks

H/W Trojans
Physical Attacks in Dimensions

Objective: Securing crypto-engines in the areas of ICs

Safety zone at IC chip

Magnified 5mm

Leakage observed on PCB
~100mm

Leakage through far EM emanation
1m~
Physical Attack Isolation Walls at Chip Level

Active attack

Passive attack

Plain text, Cipher text, Secret key

Core clock

Cryptographic device

Data I/F

Cryptographic processor

 PMC

 PLL

Core \( V_{DD} \)

Core \( V_{SS} \)
Passive Attack -- Power Noise Analysis

Analysis models (Attacker)
- Simple power analysis (SPA)
- Differential power analysis (DPA)
- Correlation power analysis (CPA)
- Local EM analysis (LEMA)

µEM probe (Attacker)

IC chip with crypto engine

EM emanation

Package and PCB
Active Attack -- Laser Fault Injection

- High resolution fault injection both in time and space, 1-bit fault potentially leads to leakage of 121-bit key (@AES-128)
## Attack Measures and Packaging Structures

**Physical media**

<table>
<thead>
<tr>
<th>Type</th>
<th>Attack Type</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive attacks</td>
<td>Side channel attack (SCA)</td>
<td>EM, Photon, Volt., Current</td>
</tr>
<tr>
<td>Active attacks</td>
<td>Fault attack (FA)</td>
<td>EM, Laser, ESD, Glitch</td>
</tr>
</tbody>
</table>

**Assembly structure**

<table>
<thead>
<tr>
<th>Type</th>
<th>Process</th>
<th>Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIC</td>
<td>Wire bonding, Flip chip</td>
<td>Plastic mold, CoB, etc.</td>
</tr>
<tr>
<td>FPGA</td>
<td>3D stacking, Fan out</td>
<td>Si interposer, MCM, etc.</td>
</tr>
</tbody>
</table>
Outline

Physical attacks

- On-chip security sensor circuits
- Simulation technique of side-channel leakage
- Conclusions
EM observation impossible w/o disturbance to fields -- "invasive attack" is not true
LEMA Sensor Features

- No frequency reference needed
  - Robust and yet low-cost countermeasure
  - Different coil shapes further enhance robustness
  - Dual EM-probe attack almost impossible

- Fully-digital oscillator-based sensor circuit
  - Detection: 2 Racing Digital Counters (2RDC)
  - Calibration: Ring Oscillator (RO) + 2RDC

Design Example

Crypto Core (e.g. AES)

S-BOX[0:7] S-BOX[8:15]

Sensor Core Circuit

4-Turn Coil $L_1$
3-Turn Coil $L_2$

Supply-Current Equalizer

128bit Composite-Type AES Cryptographic Core

Dual sensor coils
Detection Range Measurements

<table>
<thead>
<tr>
<th>Probe-to-Chip Distance Z [mm]</th>
<th>fLC Shift [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>fLC1</td>
</tr>
<tr>
<td>0.05</td>
<td>fLC2</td>
</tr>
<tr>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>0.15</td>
<td></td>
</tr>
<tr>
<td>0.2</td>
<td></td>
</tr>
</tbody>
</table>

Micro EM Probe
128bit AES Chip
Demonstration of EM Probe Detection

3-Turn Coil $L_2$

4-Turn Coil $L_1$

No Probe Approach

Probe Approach to $L_1$

5.2% Shift

1/4 Divided Clock Frequency Spectrum
LFI Attack Sensor

Distributed Bulk-Current Sensor

Sensor Array

Sensor Frontend [286F^2/Cell]

Crypto Core w/ Distributed Sensor

Wired OR

Sensor Back-End
LFI Detection Measurements

LFI Detection Sensor Demonstration

LFI Detection Sensor Demonstration Movie
Outline

Physical attacks
On-chip security sensor circuits

► Simulation technique of side-channel leakage
► Conclusions
Side-Channel Analysis

- Analysis (or attacks in a malicious case) to extract a secret key from power-noise waveforms
- Simulation technique to evaluate security risks in design against diversified leakage models

Simple Power Analysis (SPA)

- Crypto computation on scalar multiplication algorithm (e.g. point doubling, point addition)
- Power noise during encryption

Correlation Power Analysis (CPA)

- Voltage range to correlate with internal activity with Hamming distance between before and after the crypto computation
- Power noise voltage drops at the clock cycle of interest

- Voltage drop
  - Time(ns)
  - Voltage drop (a.u.)
  - Hamming distance

- Cypher text #1
- Cypher text #2
- Cypher text #10000

- Guessed key

\[ I(t) \]

\[ \text{Crypto computation on scalar multiplication algorithm (e.g. point doubling, point addition)} \]

\[ \text{Power noise during encryption} \]

\[ \text{Guessed key} \]
CPS* Model for Diagnosis and Analysis

*Chip-Package-System board

Full-system level simulation of power-noise SC leakage
Challenges

► **Challenge1**: Chip Package System (CPS) board-level power-noise SC leakage modeling and simulation

- Side-channel leakage is assessed on countermeasure crypto ICs in a design phase.

► **Challenge2**: Analysis (attacks) by simulation to derive a secret key from IC chip level power noise waveforms

- **Public-key cryptography** – Simple Power Analysis ("SPA"), a single power-noise waveform over thousands of CLK cycles, very long time power noise simulation is required.

- **Private-key cryptography** – Correlation Power Analysis ("CPA"), power-noise waveforms for thousands of different plain texts, very large set of power noise simulation is required.
Chip Power Model of Crypto Engines

Noise paths and noise sources

(1) Full chip PDN modeling
- include silicon substrate
- w/o dynamic power simulation

(2) Core level power modeling
- w/o full chip Si sub. and PDN extraction

Power-noise SC leakage simulation

Case 1: Private-key (e.g., AES) - power-noise waveforms for thousands of plain texts (#1~#10000)
(different test vectors for short CLK cycles)

Case 2: Public-key (e.g., RSA, DSA, ECDSA) -- a single power-noise waveform of several thousand CLK cycles
Silicon Experiments

► 128bit AES crypto IC chip
  ✓ 3 mm x 4 mm
  ✓ 130 nm CMOS process
  ✓ Private key cryptographic (AES)
  ✓ Single power domain (1.5V)

► Evaluation board and system
  ✓ 7.3 cm x 10.0 cm
  ✓ 4 layers of interconnect
  ✓ Chip on Board (CoB) assembly
  ✓ Daughter board to micro controller
Power-Noise SC Leakage Simulation Results

Case study: private-key cryptographic IC chip
- AES encryption engine
- Operation frequency: 34 MHz

<table>
<thead>
<tr>
<th># of cells</th>
<th># of wires</th>
<th># of vias</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full IC chip</td>
<td>231036</td>
<td>13674</td>
</tr>
</tbody>
</table>

Active gate count=34K

Power noise on VDD during crypto operation of last round (12 ns) in C-P-S simulation
- # of plain texts: 1500

Simulation cost evaluation
- server: Intel Xeon CPU ES-2699 v4 (2.2GHz)

<table>
<thead>
<tr>
<th></th>
<th>Memory</th>
<th>Threads</th>
<th>CPU time</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDN modeling</td>
<td>2726MB</td>
<td>8</td>
<td>3.0 hour</td>
</tr>
<tr>
<td>power noise modeling</td>
<td>2348MB</td>
<td>8</td>
<td>8.5 min</td>
</tr>
<tr>
<td>power noise simulation</td>
<td>229MB</td>
<td>1</td>
<td>2.8 sec</td>
</tr>
</tbody>
</table>

For a single waveform
Traditional full-chip level simulation takes longer computation time due to impedance extracted from physical layout of an IC chip in long sim. time.

Proposed flow iteratively updates the active part of CPM while keeping passive networks (e.g. PDN) and focuses on dynamic power noise data.
Summary

- Exploration of on-chip protection circuits against a variety of physical attacks in passive and active manner.
- Chip-package system board simulation technique toward the design of crypto circuits for resiliency, and also to design of attack sensors.
- Research spaces of on-chip protection against H/W Trojans.

Acknowledgments: The authors would like to deeply thank Dr. Norman Chang for collaborative research works on SC leakage analysis, and Profs. Noriyuki Miura, Naofumi Homma, Yuichi Hayashi and Kazuo Sakiyama for scientific discussions.