The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance

~Panel Discussion~

Verification & Test on LSI design

Takeshi Fujino @ Ritsumeikan Univ.
Yohei Hori @ AIST
Masaya Yoshikawa @ Meijo University
Daisuke Suzuki @ Mitsubishi Electric
LSI and Security Functions

- The DEPENDABILITY of the system strongly dependent upon the SECURITY
  - Security functions are implemented in LSI in most cases.

- Electronic Toll Collection (ETC) for Expressways
- Car Security (Key, Intra and inter network)
- Smart Meters (with HEMS)
- Battery Authentication
Security Functions and Cryptography

Cryptography for Realizing Security Functions (exam.)

1. **Authentication**: Read/write permissions to HDD are granted to proper users
2. **Encryption**: HDD are encrypted in case of loss or theft

The employed cryptography is designed so that it does not leak any information of authentication or encryption keys even if communication data is eavesdropped.
The Information Leakage from Crypto module

- Mathematical Cryptanalysis to regular Input/Output is examined by Cryptographer
- Cryptanalysis utilizing Physical Information: responsible to LSI Designer
  - Ex. Side Channel Attack / Fault Attack
Tamper Resistant Cryptographic Module have been developed

- Standard Cryptographic ASIC provided with SASEBO-R board
- DES Cryptographic Module using Domino RSL gate
- AES Cryptographic Module using Dual-Rail RSL Memory
The verification method of SCA resistance

**Conventional LSI Design Flow & Power Simulation**

- **System Design**
  - Power simulation = A few minutes

- **Logic Design**
  - Power simulation = Several hours

- **Layout Design**
  - Power simulation = A couple of days

More than **1,000,000** power consumption waveforms are required for SCA verification. => Several thousand years? are required.

*The speed and accuracy of power simulation method*

<table>
<thead>
<tr>
<th>Tool</th>
<th>SPICE</th>
<th>Prime Time PX</th>
<th>FPGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Low</td>
<td>Middle</td>
<td>High</td>
</tr>
<tr>
<td>Accuracy</td>
<td>High</td>
<td>Middle</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*1 Dedicated logic gate/circuit (RSL, D.R. Memory etc.) for DPA countermeasure is difficult to be applied to Prime Time.

*2 The power consumption characteristic of FPGA is different from that of ASIC.

There is **no good SCA verification method** which improves a trade-off between speed and accuracy.
The Test of Cryptographic Module

- Normal Function Test
  - Verify the expected output is returned for Input Test Fixture
  - Standard Logic Tester is used

- Security Function Test
  - Confirm the secret information is not revealed to any Side Channels (Output Timing, Power, Electromagnetic Field) under any Operating Conditions (Fault Attack, Invasive Attack)
  - Special Equipment must be prepared
Dependable VLSI

SASEBO: Side-channel Attack Standard Evaluation BOard

- Provides a common experimental environment of SCA to more than 100 academic, industrial and governmental institutes in the world.
- Contributes to find new threats and develop proactive countermeasures (e.g., fault sensitive analysis, fault behavioral analysis, SCA against hash function or PUF...)
- About 170 academic papers using/citing SASEBO (25/May/2012, Google scholar)

- For cryptographic ASIC evaluation (QFP160)
  - Customize daughter board for specified ASIC in low price (Board Design data are open for academic)
  - Low noise

- For cryptographic FPGA evaluation
  - Equipped with a Xilinx 28-nm Kintex-7 FPGA
  - SCA evaluation on the state-of-the-art process
  - Sufficient logic resource for implementing complicated countermeasures
  - Suitable for security evaluation of an integrated system composed of crypto cores, networks and applications.

Ver. Ritsumeikan Univ. (QFP80)
Development of SCA Environment

【DPA Environments】

- Documents including “Quick Start Guide” for DPA using SASEBO
- Automatic data analyzer
  - Can be used without special skills or knowledge of SCA
  - Realize fair verification among various certification institutes in the world

【DEMA Environments】

- Compact automatic EM scanner for effortless EMA
  - Range of movement: 50mm (3 axes)
  - Positional accuracy: less than 100 um
- High performance EM probe
  - 10-turn φ1.6mm coil
  - Frequency characteristic: 1 GHz
  - Spatial resolution: 0.45 mm