The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance

Focusing on the security of hardware modules
- Tamper resistant cryptographic circuit
- Evaluation tools for tamper resistance
- Physical Unclonable Function (PUF)

Takeshi Fujino @ Ritsumeikan Univ.
Yohei Hori @ AIST (Advanced Industrial Science and Technology)
Masaya Yoshikawa @ Meijo University
Daisuke Suzuki @ Mitsubishi Electric
Contents

- Introduction to cryptographic modules and Side channel attacks
- The aspect of Side channel attacks (SCAs)
  - The Effect of on-chip Capacitance
  - The Effect of on-chip Metal Shielding
  - The Effect of finer device fabrication process
- The AES cryptographic circuit against SCAs
  - Countermeasure against Power Analysis
  - Countermeasure against EM Analysis
- The evaluation platform SASEBO
  - Smartcard-type evaluation board new
- Secure Key Storage using Physical Unclonable Functions
1. INTRODUCTION TO CRYPTOGRAPHIC MODULES AND SIDE CHANNEL ATTACKS
The research target in tamper resistant security LSI

- The design methodology for tamper resistant LSI
- The evaluation tools for tamper resistance
- Secure system utilizing Physical Unclonable Function

Fault Attack
- Illegal Clock (e.g. Glitch)
- Power Supply fluctuation
- Input Noise

Malicious Input
Abnormal Output

Regular Input/Output

Security LSI module

Side Channel Information
- Processing Time
- Current/Voltage
- EM Radiation

Invasive Attack
- Open Package
- Laser or EM Injection
- Reverse Engineering
- Probing electro signal

Cloning Attack

Side Channel Attack
Cryptographic module and Side Channel Information

- Cryptography for Realizing Security Functions (exam.)
  ① Authentication: Read/write permissions to HDD are granted to authorized users
  ② Encryption: HDD data are encrypted in case of loss or theft

[Diagram showing authentication and encryption processes]
Side Channel Attack

- Secret key is revealed by exploiting side channel information from crypto module
- Consumption Power or EM leakage are used as an information

Evaluation Board SASEBO-RII

Plain Text

Control & Analysis software for revealing secret key

Cipher Text

Oscilloscope

AES Chip

EM Probe

Power

Cryptographic Module

Secret key is revealed by exploiting side channel information from crypto module

Consumption Power or EM leakage are used as an information

AES Chip
Dependable VLSI
Tamper Resistance

The attacking points on AES crypto circuit

- **Hamming Distance (HD)**
  - Data Register

- **Hamming Weight (HW)**
  - Sbox input/output

- **Power consumption is correlated to the HD of resisters and HW of Sbox input**
2. THE ASPECT OF SIDE CHANNEL ATTACKS
The Effect of Capacitance

- The Power leakage is considered to be reduced by the on-Chip or off-chip decoupling capacitor.
- On-chip Capacitor make vulnerable to EMA attack with HW correlation.

SAMPLE: Non-countermeasured AES (Sbox:Composite Field)
The Effect of Metal Shielding

- The Metal Shielding reduce the EM leakage
- The secret key can still be exploited by the increased number of traces
- Metal Shielding is not a perfect solution against EM attack

SAMPLE:
I/O masked dual rail ROM
(The countermeasured AES circuit against Power Analysis)
The Effect of Finer fabrication process

- The Power and EM attack are tested in 65 and 28nm FPGA
- EM attack getting powerful in the finer process
  - Reason: Static Power leakage is dominant

![Graph showing the effect of finer fabrication process on EM and Power attacks.](image)

- Kintex-7 (28nm)
- Virtex-5 (65nm)
3. THE AES CRYPTOGRAPHIC CIRCUIT AGAINST SCAs
(Our countermeasure) I/O Masked Dual Rail ROM (MDR-ROM)

- MDR-ROM provides constant power consumption irrespective of input value
- 2K bit MDR-ROM is used in the SubByte transformation on the AES circuit
- Other linear circuits are masked by the additive mask

IO-masked dual-rail (MDR) ROM

Advanced Encryption Standard (AES)
I/O Masked Dual Rail ROM (MDR-ROM)

- MDR-ROM provides constant power consumption irrespective of input value.
- 2K bit MDR-ROM is used in the SubByte transformation on the AES circuit.
- Other linear circuits are masked by the additive mask.

**MDR-ROM**

- MDR-ROM provides constant power consumption irrespective of input value.
- 2K bit MDR-ROM is used in the SubByte transformation on the AES circuit.
- Other linear circuits are masked by the additive mask.
Evaluation results of MDR-ROM

- Dual rail RSL memory is used for S-box and other circuits are designed in Standard ASIC flow
- Power overhead is 50% of no countermeasure
- Sufficient PA resistance is demonstrated compared with other countermeasures (WDDL, MDPL, MAO, TI)
EM leakage on MDR-ROM

- MDR-ROM demonstrate high resistance against Power Attack
- MDR-ROM has a EM leakage called “Geometric Leak”
- This type of leakage is discovered for the 1st time in the world on our experiments (presented at CHES 2013, invited to submit on Journal of Cryptographic Engineering)
Multiplicative masking is also introduced in addition to additive mask

Inverse operation on Galois Field is tabled on the MDR-ROM

The addresses except for zero are randomly accessed regardless of the input data

Sbox is commonly used for encryption and decryption

The number of MDR-ROM is half
EMA resistance on HMDR-ROM

- Geometric leakage is diminished and high EMA resistance is obtained in HMDR-ROM

Additive mask: OFF
Multiplicative mask: OFF

Additive mask: ON
Multiplicative mask: OFF

Additive mask: ON
Multiplicative mask: ON
4. THE EVALUATION PLATFORM

SASEBO
Development of SCA Test Environment

• **SASEBO**: Side-channel Attack Standard Evaluation Board
  – Provides a uniform experimental environment to academic, industrial and governmental researchers
  – Facilitates research of side-channel attacks

• **Outcome**
  – Commercially available and globally used in >100 institutes
  – >1100 academic papers use/cite SASEBO (1/Nov/2013, Google scholar)
  – Included in world’s de-facto standard SCA evaluation tools
MiMICC: Micro Measurement IC Card

- Smartcard-type evaluation board w/ 45-nm FPGA
  - H/W-implemented cipher algorithms (etc.) on a smartcard can be tested
  - Physical dimensions are almost ISO/IEC 7810 ID-1 compliant
  - ISO/IEC 7816 (T=0) data transfer protocol is supported
EMA Demonstration Using MiMICC

- Secret key extraction from AES on the smartcard
  - Key length = 128 bits (16 bytes). Block length = 128 bits.
  - Without countermeasures

- EM radiation from the chip is measured and analyzed

AES is running on the smartcard board MiMICC.
EM radiation is measured with loop antenna.
5. SECURE KEY STORAGE USING PHYSICAL UNCLONABLE FUNCTIONs
Physical Unclonable Function

- PUF extracts physical variation in each device
- Unique and Unclonable ID (Identification code) can be produced
- We proposed arbiter base DTM PUF with high uniqueness

Challenges \[ C_0, C_1, C_2, \ldots, C_{N-1} \]
- \#1 \[ 0, 0, 0, \ldots, 0 \]
- \#2 \[ 1, 0, 0, \ldots, 0 \]
- \#3 \[ 0, 1, 0, \ldots, 0 \]

Responses
- PUF #A
- PUF #B
- PUF #C

Conventional Arbiter

DTM method (Delay time measurement)
PUF based Key Generation

- IDs produced by PUF has the instability
- Fuzzy Extractor is used for error correction

Fuzzy Extractor (FE)

Error Correction Code

<table>
<thead>
<tr>
<th>in</th>
<th>out</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
</tr>
<tr>
<td>1</td>
<td>111</td>
</tr>
</tbody>
</table>

Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data
Secure Key Storage using PUF

- Authentication key had to be stored in secure memory
- PUF Encrypted authentication key (2) can be stored in the standard memory
- Authentication key can be produced by (1) (2) (3)

Initial Key Generation

1. Challenges → PUF
2. RNG → ENC
3. DEC → ENC → Hash
   - PUF Key

Authentication Key cannot be produced without PUF
SUMMARY

- Side channel attacks (SCAs) is a serious threat for cryptographic modules which are used in IC card, smart meter or automobile

- The countermeasures against SCAs is not easy
  - On chip capacitor is effective against power analysis but vulnerable against EM analysis
  - Metal Shielding is not perfect countermeasure against EM analysis
  - EM analysis is still powerful on finer device fabrication process

- The AES cryptographic circuit against SCAs are designed
  - I/O Masked Dual Rail ROM (MDR-ROM) is a good countermeasure against power analysis, but EM leak called “geometric leak” was found
  - Hybrid Masked Dual Rail ROM (HMDR-ROM) is free from “geometric leak”

- The FPGA on the smartcard is newly designed, and EM analysis is successfully demonstrated by using SASEBO-W board

- Stable PUF Key generation by Fuzzy-Extractor, and authentication system using PUF-protected key are demonstrated