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
Masaya Yoshikawa @ Meijo University
Daisuke Suzuki @ Mitsubishi Electric
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 are encrypted in case of loss or theft

1. **Authentication**: Read/write permissions to HDD are granted to authorized users
   - Authorized User

2. **Encryption**: HDD are encrypted in case of loss or theft
   - Security Functions (LSI)
   - Storage (HDD)

**Side Channel Information**
- Processing Time
- Current/Voltage
- EM Radiation
Side Channel Attack (Differential Power Analysis)

- Secret key is revealed by exploiting power traces from crypto module
- The evaluation tools are also developed in this project

Evaluation Board: SASEBO-RII

- Plain Text
- Cipher Text
- Control & Analysis software for revealing secret key

Power Monitoring

Other Evaluation Boards (FPGA):
- SASEBO-GIII
- ZUIHO

Compact Scanner for EM Analysis
DPA resistant AES circuit using dual-rail RSL memory

- 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 DPA resistance is demonstrated compared with other countermeasures (WDDL, MDPL, MAO, TI)
Physical Unclonable Function for anti-counterfeiting

- PUF exploit the random process variations which make each chip unique and unclonable
- The authentication using PUF is useful for anti-counterfeiting
- RG-DTM Arbiter PUF, Glitch PUF, and PL PUF are developed

Glitch PUF

Non-linear Random Logic
Glitch Generation

Generate response according to generated number of glitches

Input Resister

LSI #1
LSI #2
LSI #3

Dinit SEL
Din
Dout

LFSR_core

1 2 3 → 0
1 2 → 1