The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance

Tamper Resistant VLSI Design
Two methods are under development

(1) Domino RSL Gate
Output Transition Probability is uniformed by changing logic function by random number r

(2) Dual Rail RSL Memory

Evaluation Results of DES
Number of Traces vs. Number of Revealed Key (bits)

DES Cryptographic Circuit (180nm)

Evaluation Tools for Tamper Resistance
- SCA Evaluation Board and EM stage are commercially available

Unclonable Function
Arbiter PUF * using RG-DTM method

- Generate Unique ID from device variability under device fabrication

*PUF (Physical Unclonable Function)

RG-DTM-PUF(180nm) using delay Time Measurement
- High Uniqueness
- Moderate Stability

Evaluation Results of AES Cryptographic Circuit (180nm)

AES Cryptographic Circuit (180nm)

Unmask Data Mask Data
Randomly Switched I/O

Arbiter Circuit
Challenge C1 C2 C8
Response 0 1

Conventional Arbiter
Arbiter using Delay Time Measurement

Number of Traces
0 1 10 100 1,000 10,000 100,000 1,000,000

Number of Revealed Key (bits)
0 1 2 3 4 5

Stability: Smaller HD is better
Uniqueness: Smaller Deviation is better

- Standard Evaluation Cryptographic LSI using 65nm CMOS process
- Side Channel Evaluation Board SASEBO-RII
- Scanning Stage for evaluating Electro Magnetic Field

Two methods are under development

- Normal DES
- Domino-RSL DES
- Random number generator

- In/Out controller

Number of Revealed Key (bits)
0 1 2 3 4 5

Challenge C1 C2 C8
Response 0 1

Conventional Arbiter
Arbiter using Delay Time Measurement

RG-DTM-PUF(180nm) using delay Time Measurement
- High Uniqueness
- Moderate Stability

Stability: Smaller HD is better
Uniqueness: Smaller Deviation is better