

The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance

(1) Domino RSL

Output Transition Probability is uniformed by changing logic function by random number r

Tamper Resistant VLSI Design

Two methods are under development

(2) Dual Rail RSL Memory

masked Input, masked Input, Randomly Switched I/O, masked Output

DES Cryptographic Circuit (180nm)

Evaluation Results of DES

No keys are revealed by 1 M traces

AES Cryptographic Circuit (180nm)

Unclonable Function

Arbiter PUF * using RG-DTM

- Generate Unique ID from device variability under device fabrication
- *PUF(Physical Unclonable Function)

method

Challenge C₁ C₂ C₈

Input IN, Arbiter Circuit

Response

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

Probability[%], Hamming Distance[bit]

Evaluation Tools for Tamper Resistance

- SCA Evaluation Board and EM stage are commercially available

Standard Evaluation Cryptographic LSI using 65nm CMOS process

Side Channel Evaluation Board SASEBO-II

Scanning Stage for evaluating Electro Magnetic Field