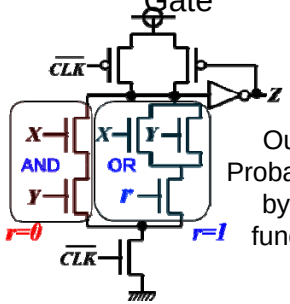
The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance

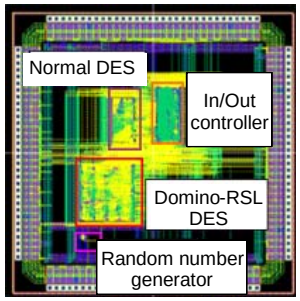
Tamper Resistant VLSI Design

Two methods are under development

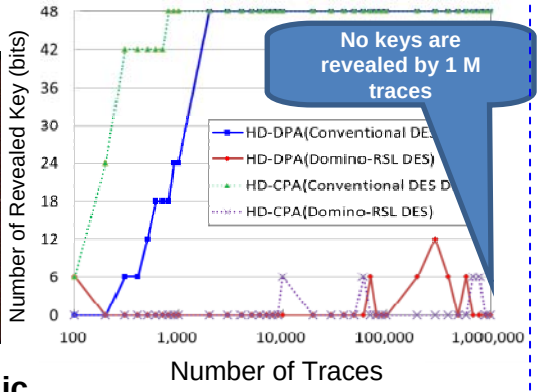
(1) Domino RSL Gate



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

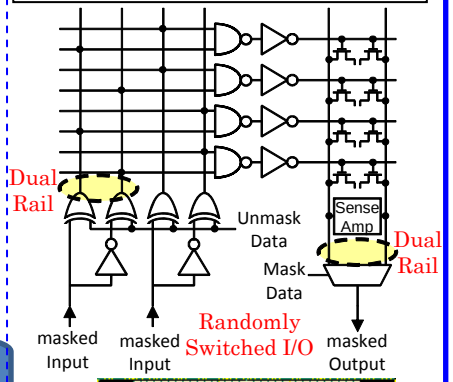


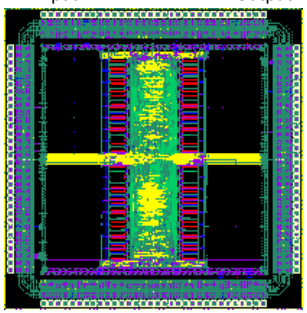
DES Cryptographic Circuit (180nm)



Evaluation Results of DES

(2) Dual Rail RSL Memory



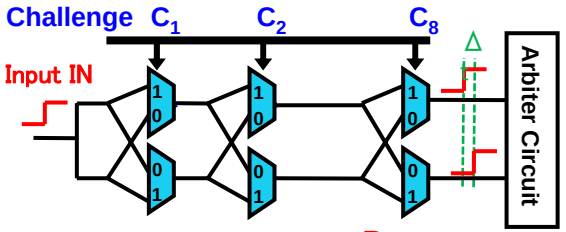


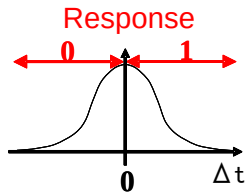
AES Cryptographic Circuit (180nm)

Unclonable Function

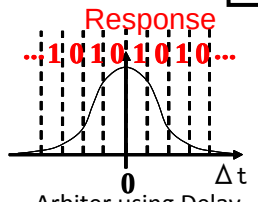
Arbiter PUF * using RG-DTM method

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

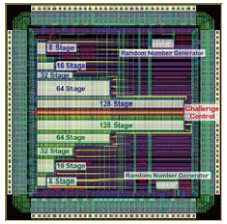




Conventional Arbiter

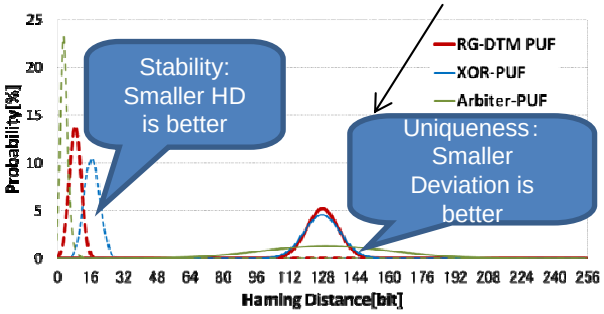


Arbiter using Delay Time Measurement



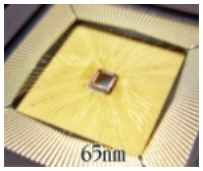
RG-DTM-PUF(180nm) using delay Time Measurement

・High Uniqueness
・Moderate Stability

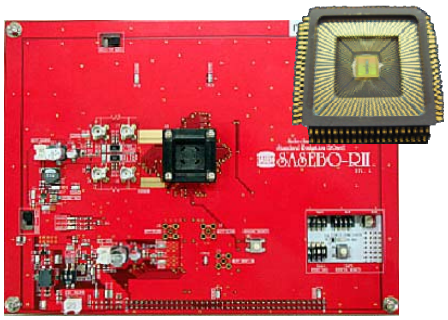


Evaluation Tools for Tamper Resistance

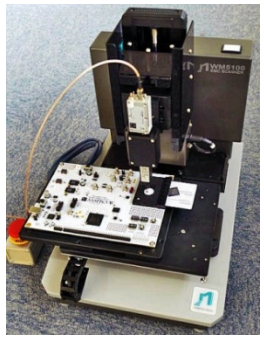
・SCA Evaluation Board and EM stage are commercially available



Standard Evaluation Cryptographic LSI using 65nm CMOS process



Side Channel Evaluation Board SASEBO-RII



Scanning Stage for evaluating Electro Magnetic Field