Hardware Security and Safety for Smart World Foundation

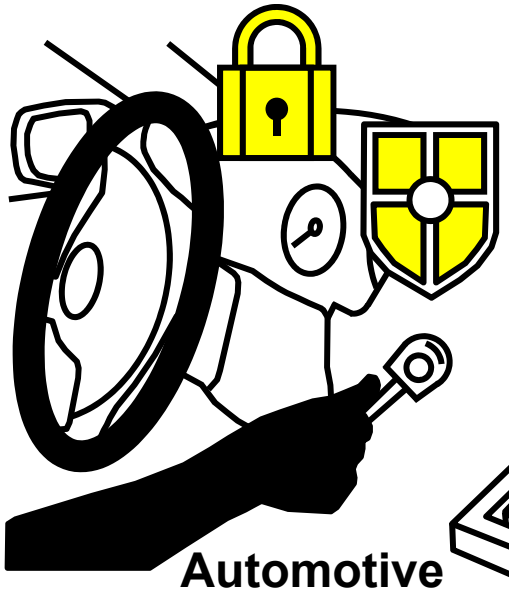
Noriyuki Miura

Graduate School of System Informatics, Kobe University

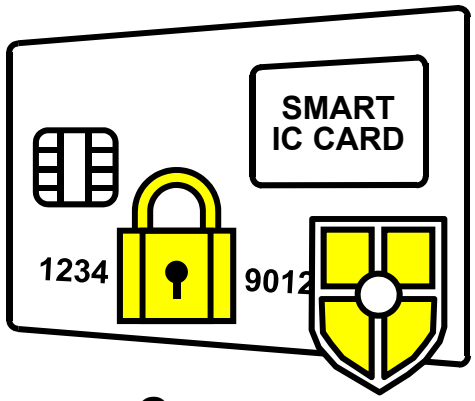
Hardware Security and Safety

►Root-of-Trust in critical applications today

Mobile
Sensor/Robot

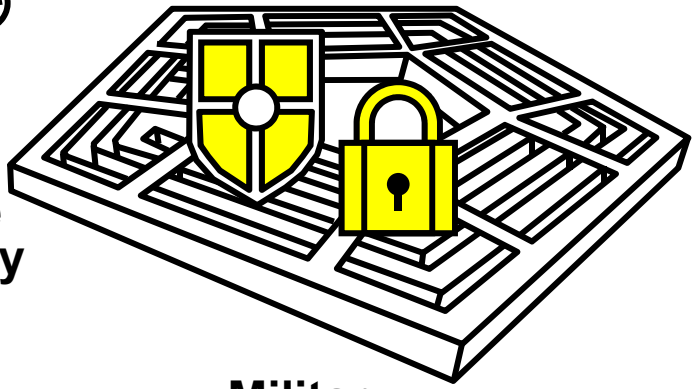


Automotive
M2M/Industry



e-Commerce
e-Authentication

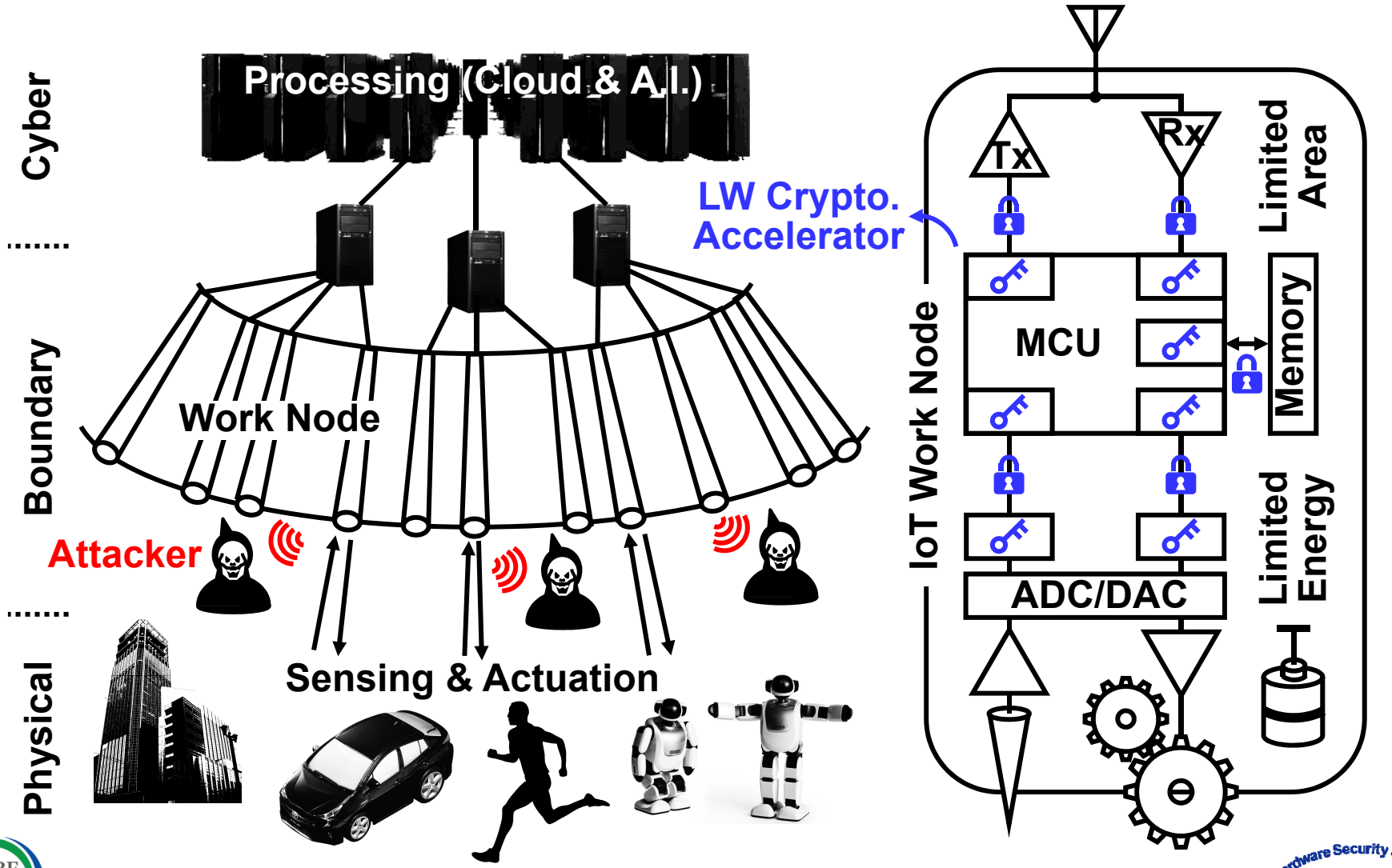
Cloud
A.I./Super Computer



Military
Defense

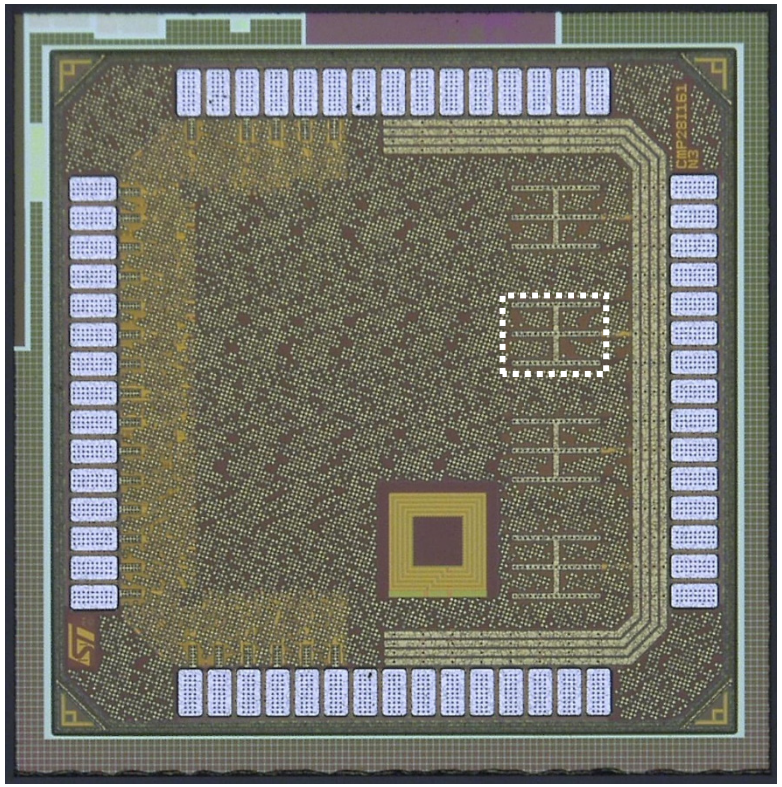
IoT Work Node Security Hole

▶Light weight HW security mandatory for IoT



Ultra-Light-Weight Cipher

- ►Light latency, energy, area performance
  - – 10x efficiency to state-of-the-art intel SMS4



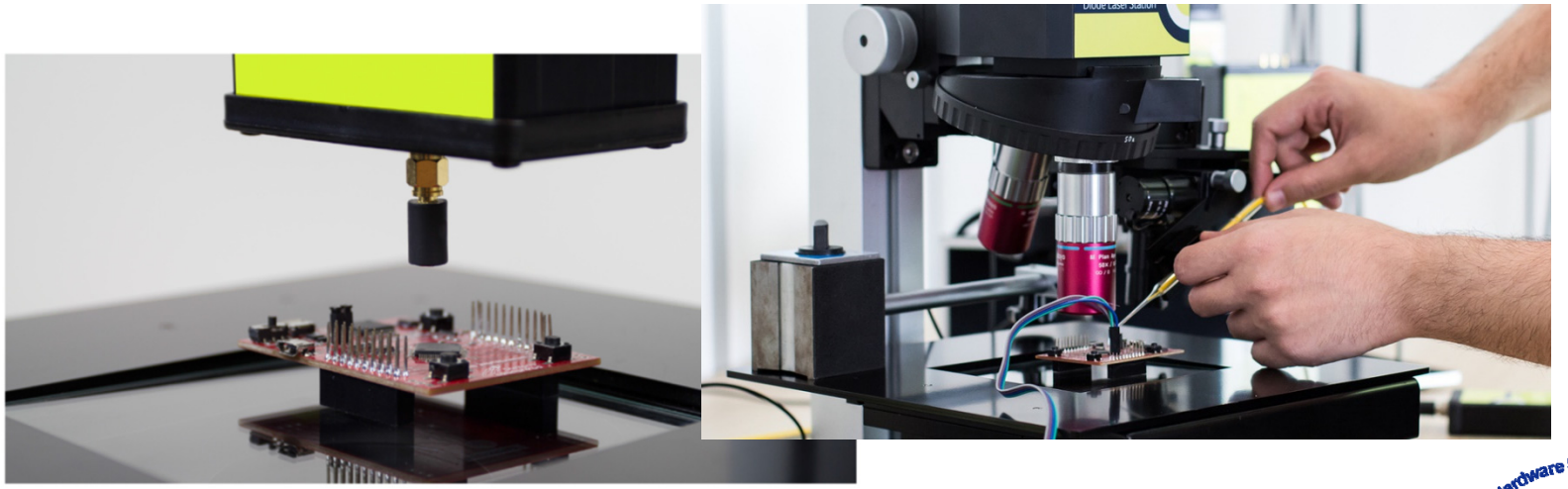
	This Work	intel VLSI'16
Algorithm	PRINCE	SMS4
Latency [ns]	5	32
Throughput [Gb/s]	25.60	4.04
Energy [pJ/b]	0.39	0.89
EDP [ns*pJ/b]	1.95 ←	28.48
Technology	28nm	14nm
Area Efficiency [μm^2/Gb/s]	289 ←	2420

[1] VLSI'17, Joint Work w/ Telecom ParisTech

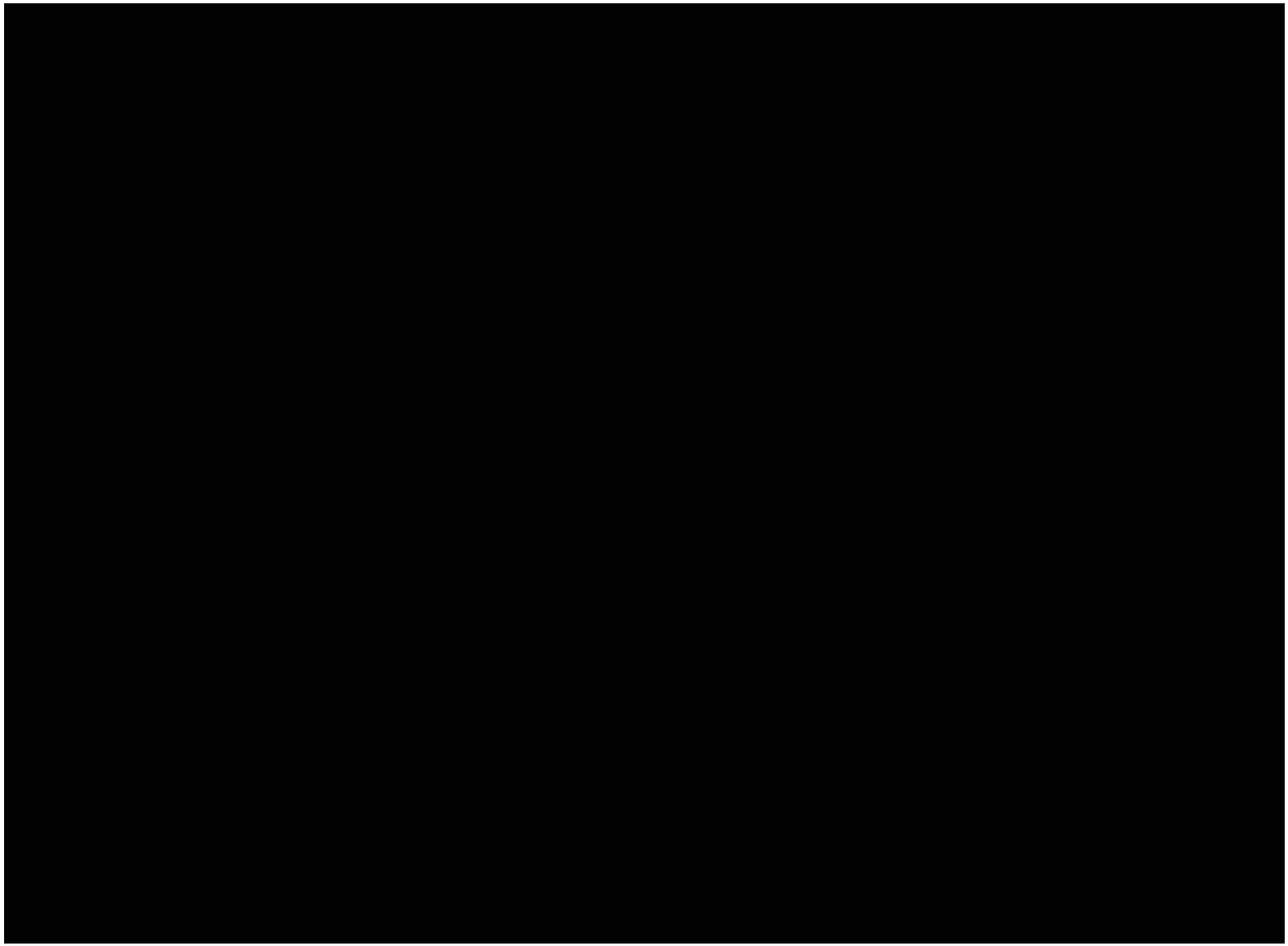
Existing Threat

- Side-channel attack exploiting EM leakage

- Fault injection attack exploiting laser



Side-Channel Attack Sensor

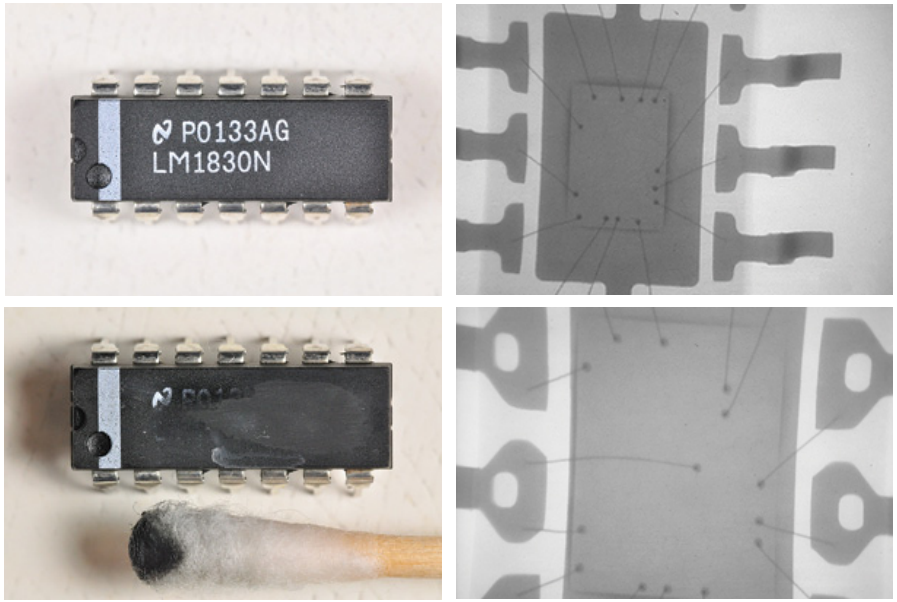


[2] VLSI'14, [3] CHES'14 Best Paper Award

Laser Fault Attack Sensor

Existing Threat

►Counterfeiting electronic devices



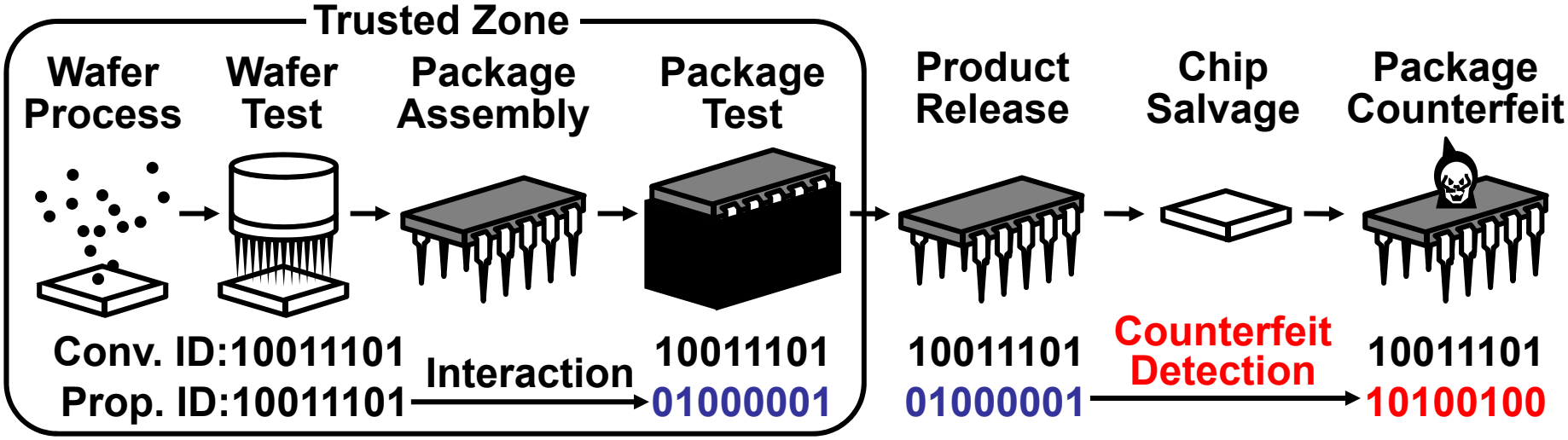
"The Hidden Dangers of Chop-Shop Electronics," IEEE Spectrum Oct.'13

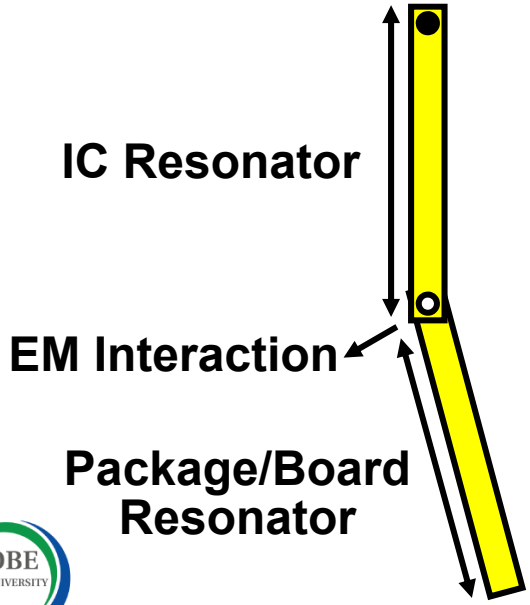
►Chip recycling, package-level manipulation

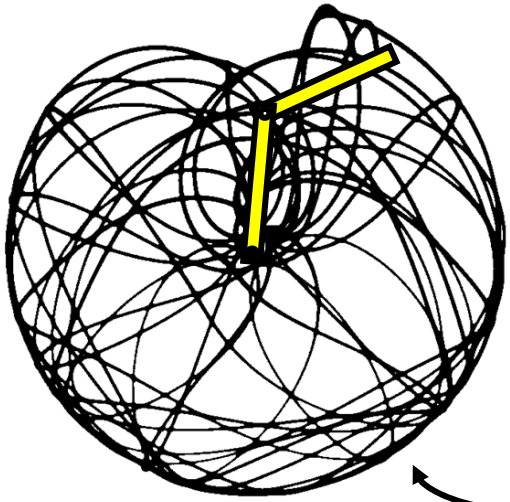
- Advanced malicious attack with low-cost
- Need countermeasure with extended traceability

Secure Supply Chain

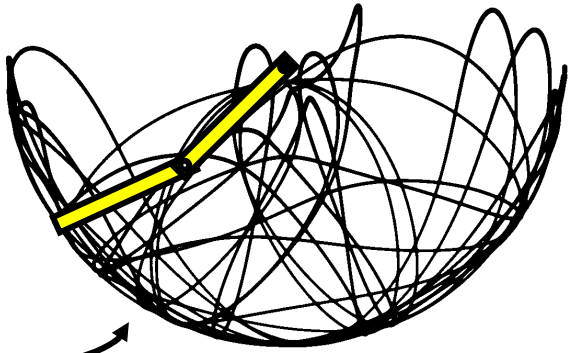
▶Extend device ID traceability for HW integrity







Chaos Oscillator Used for ID Generation



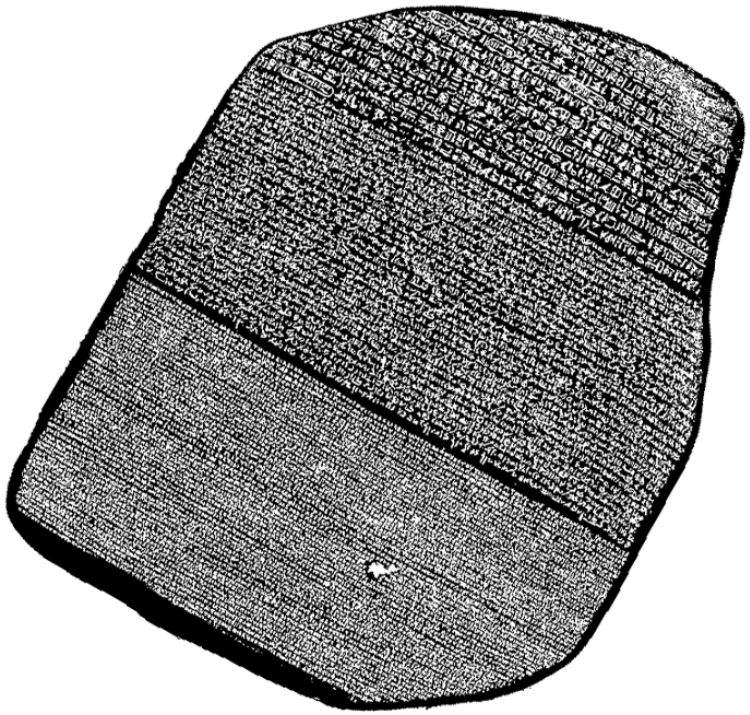
[5] A-SSCC'17

Distinguishable

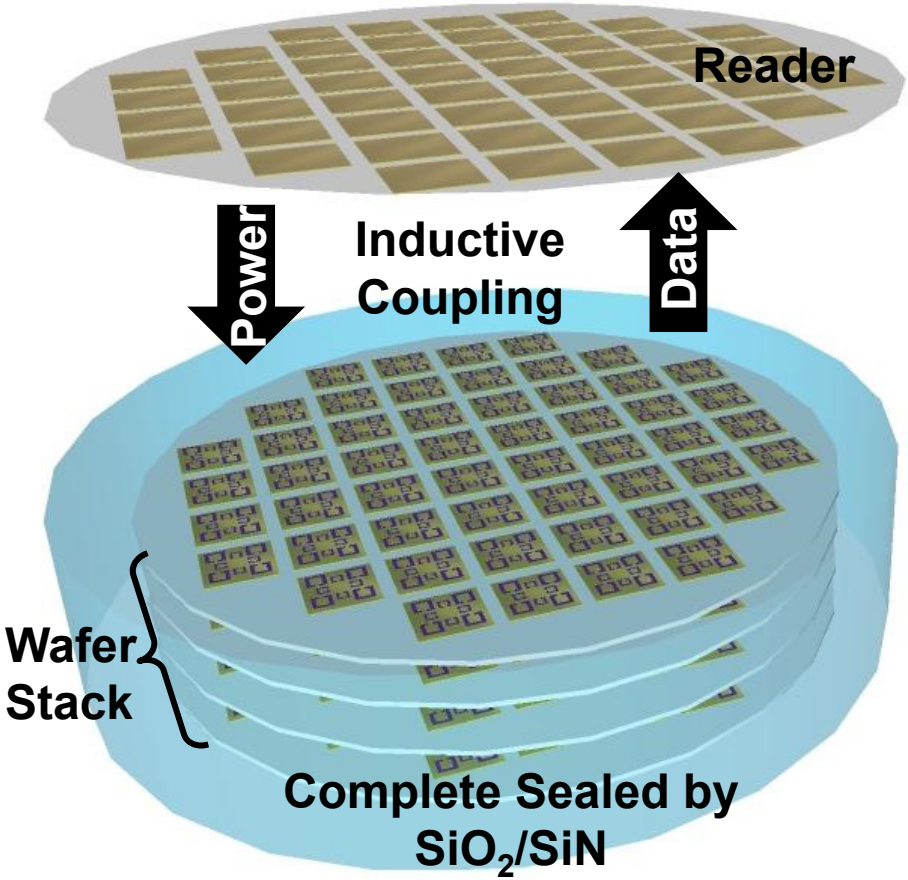
Permanent Digital Archive

►Protect information heritage for descendant

– Si-based high-density eternal storage system



Rosetta Stone
Etched Inscription
0.1kbit/inch^2



Eternal Storage Demo

Summary

- ►HW-security and safety
  - Critical in future IoT and smart society
- ►HW-level countermeasure
  - Mandatory for information root-of-trust
- ► EM engineering + slightly-analog circuit
  - Light-weight solutions for security and safety
- ►Contact information:
  - Noriyuki Miura (e-mail: miura@cs.kobe-u.ac.jp)