Physical Security Testing Workshop, Hawaii, 26-29 September 2005

Studying LSI Tamper Resistance With Respect to Techniques Developed for Failure Analysis

Tsutomu Matsumoto
Yokohama National University

Shigeru Nakajima
Van Partners Corporation

Tadashi Shibata
University of Tokyo

Atsuhiro Yamagishi
Information-technology Promotion Agency, Japan

Contents

1. Introduction

   Tamper resistance of LSI chips against physical attacks is studied from the viewpoint of LSI failure analysis.

2. Basic Physical Phenomena in LSI Chips
3. Failure Analysis Techniques

   Laying stress on the basic physical phenomena generated in LSI chips under operating conditions, we outline today's failure analysis techniques with application to evaluating or testing tamper resistance of LSI chips.

4. A Case Study of Tampering Sensor Circuits

   We give some results from our case study on inactivation of sensor circuits where emission microscopy plays an important roll.

5. A Tentative Classification of Security Levels

   Finally we show an attempt to classify the security levels for LSI chips with respect to the required equipment and the required skills of attackers.

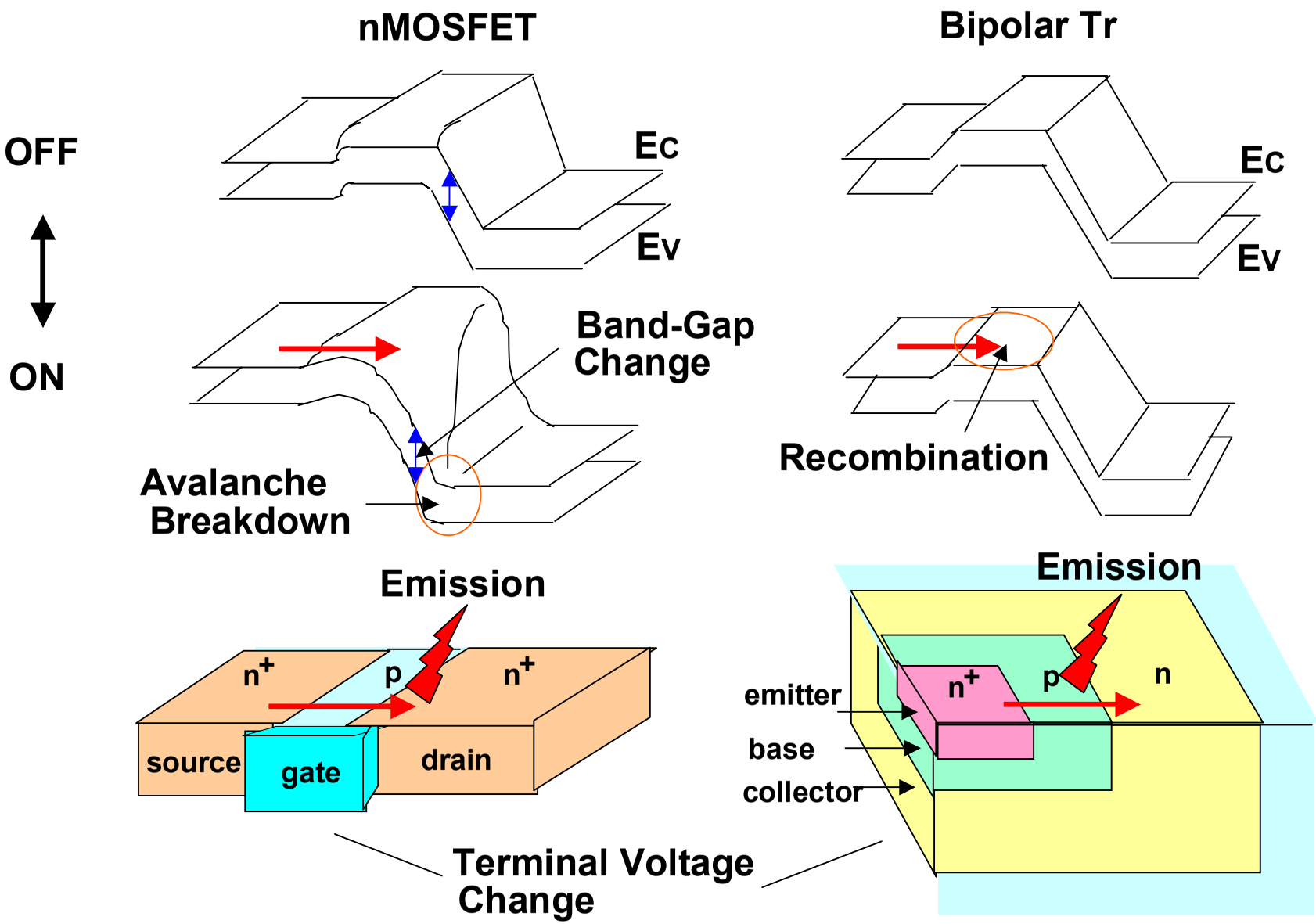
6. Summary

2. Basic Physical Phenomena in LSI Chips

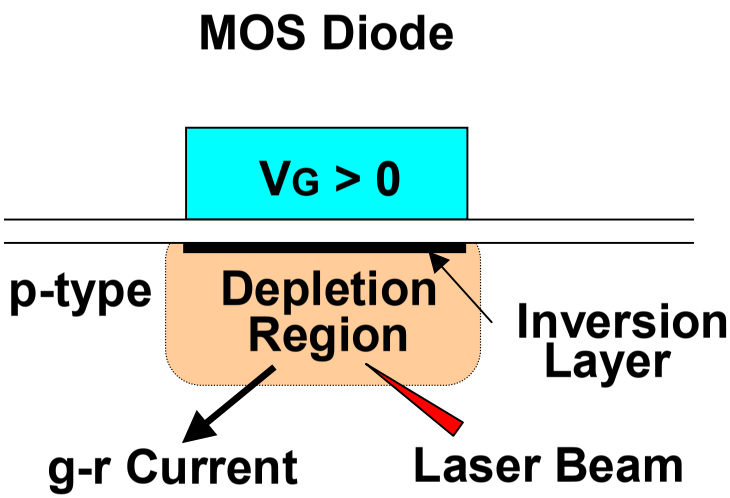
Two Classes; “Generated” and “Stimulated”

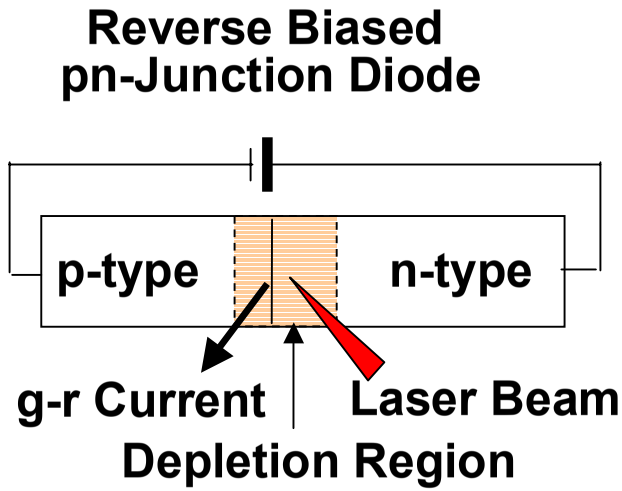
1. Generated Physical Phenomena
   - *are those generated in operating LSI chips and have three types.*
   - *The first type is band-gap narrowing in depletion region when high reverse voltage is applied to p-n junction at drain regions.*
   - *The second type is photon emission from MOSFETs and bipolar transistors by avalanche breakdown at the drain edge and recombination of holes and electrons at the base region, respectively.*
   - *The third type is terminal voltage change according to input signals.*
2. Stimulated Physical Phenomena
   - *are those induced in LSI chips by some physical stimulation.*
   - *One such physical phenomenon is excitation of carriers in depletion region by laser beam irradiation and it results in generation and recombination (gr) current flow.*

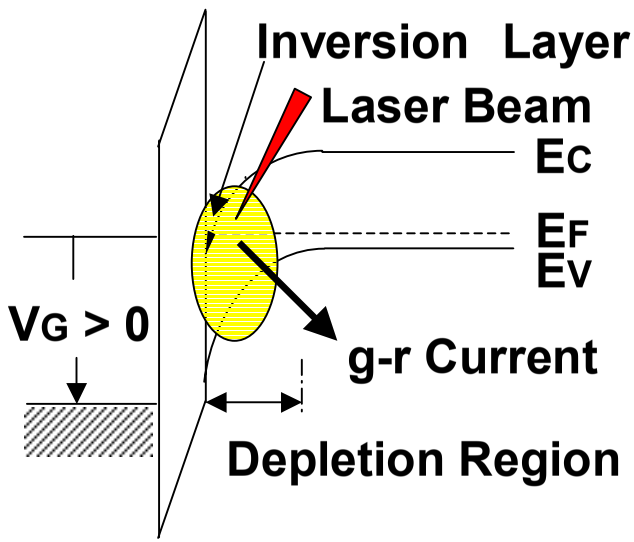
Physical Phenomena in Operating LSI

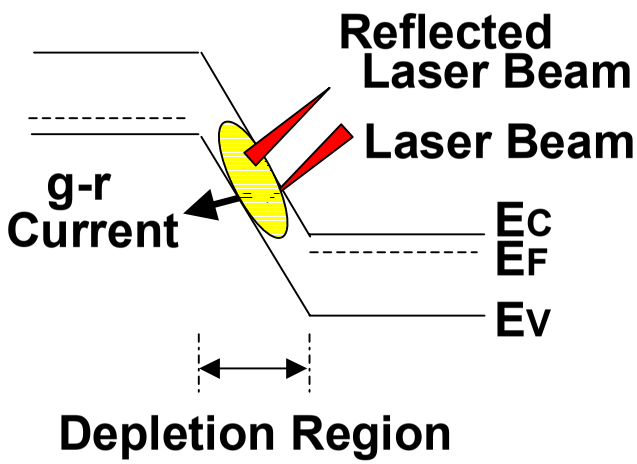


Generation-Recombination Current Flow by Laser Beam Irradiation

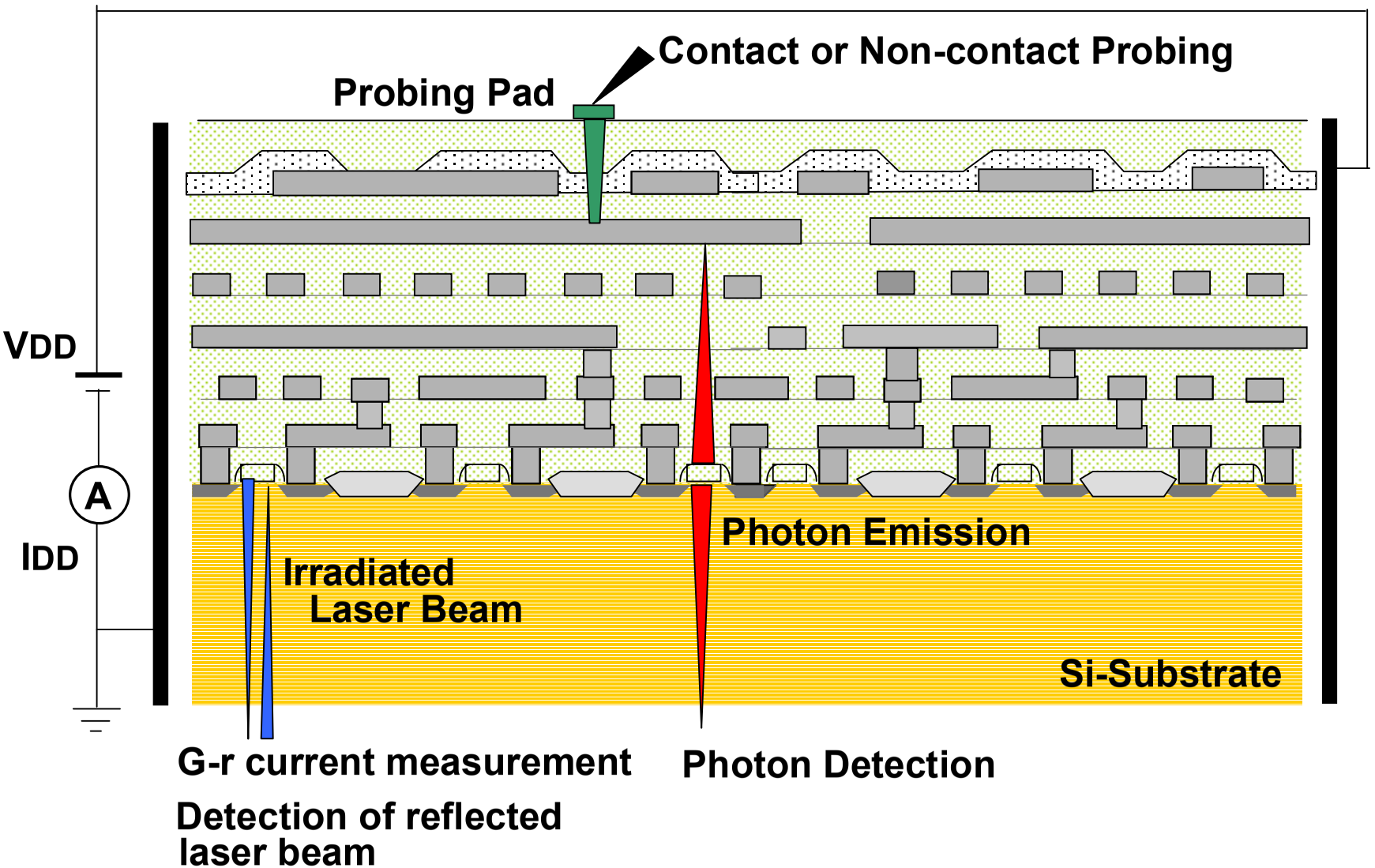




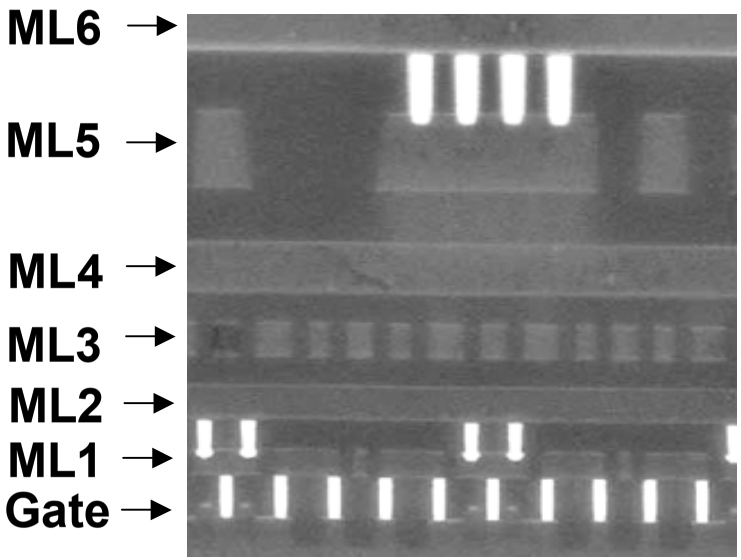




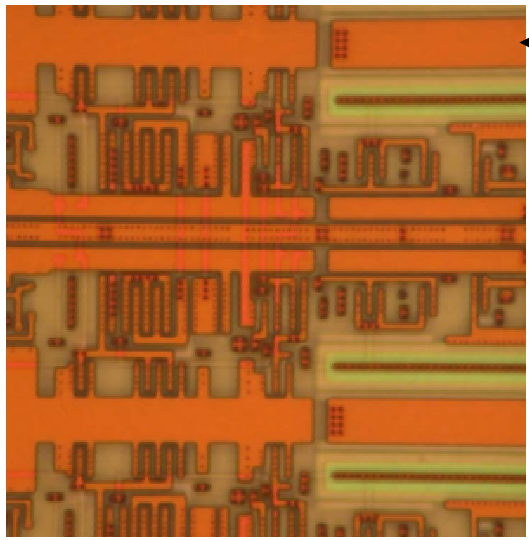
Typical Detection Methods for Physical Phenomena in LSI



Sample Preparation Techniques for Observation

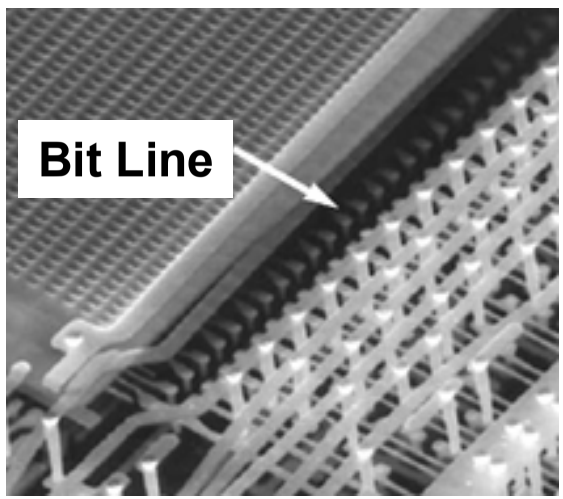


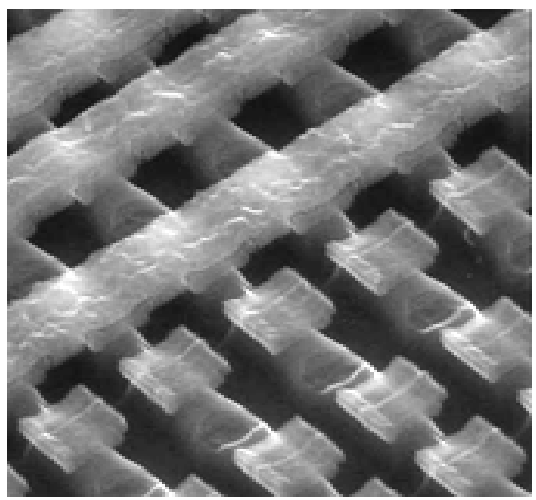
Cross-Sectioning



Physical Layer Removal

DRAM



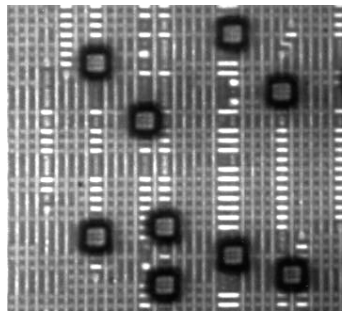


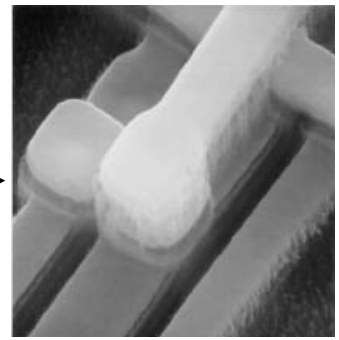
Flash Memory

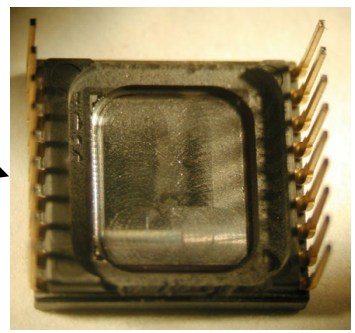
Wet Etching

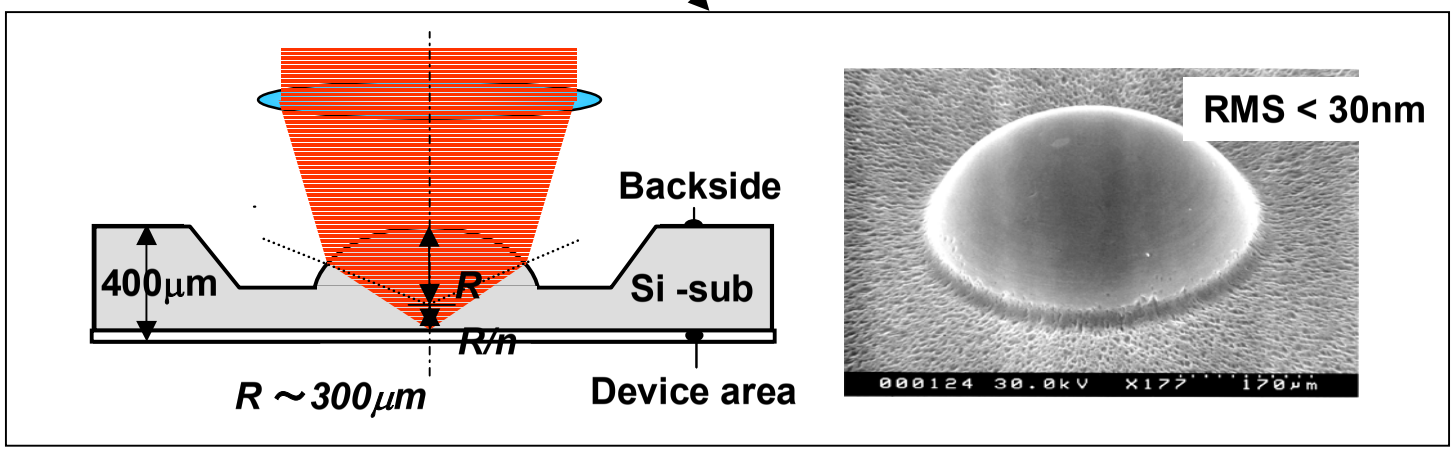
Sample Preparation Techniques for Waveform Measurements

Front-side	Pad formation
	Dielectric film removal
Backside	Si-sub thinning
	Si immersion lens formation







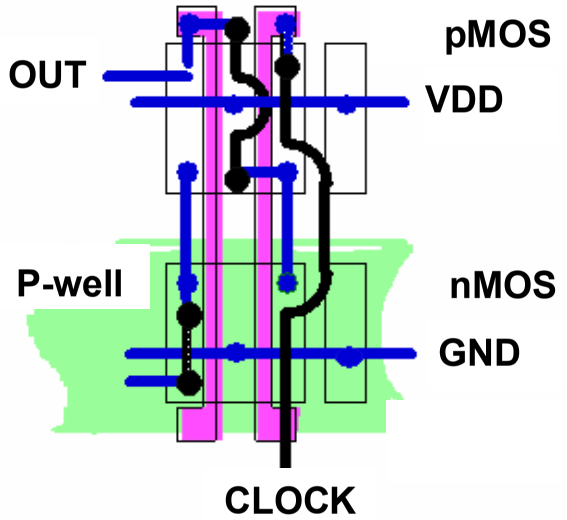


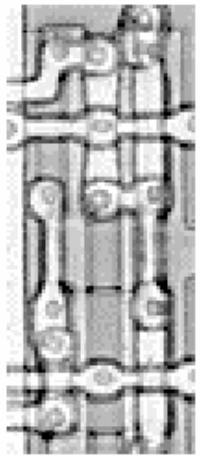
Measurement Methods for Electrical Characteristics

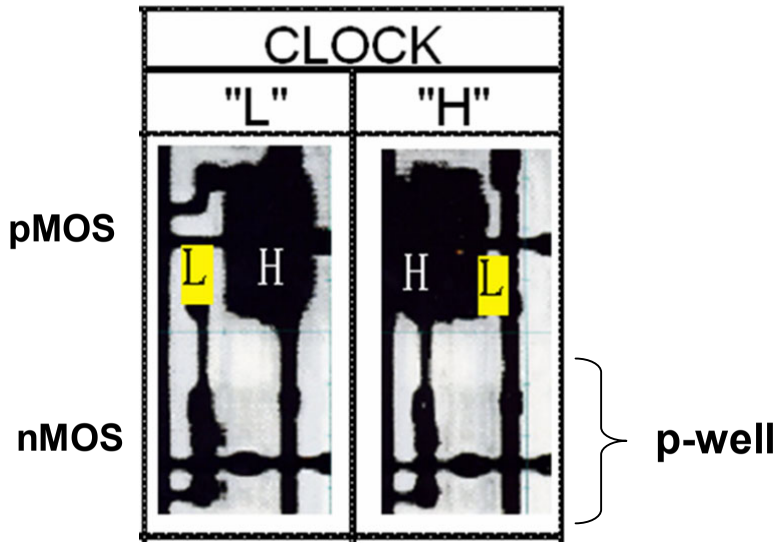
Method	Features
OBIC	Measurement of “H” or “L” state of nodes by detecting substrate current generated by laser beam exposure.
EBT	Waveform measurement by detecting amount of secondary electrons emitted from operating interconnections.
LVP	Waveform measurement by detecting intensity of laser beam reflected at reverse biased p-n junction in devices.
TRE	Waveform measurement by detecting intensity of photon emission from operating devices.
EOS	Waveform measurement by detecting polarization of laser beam after pass-through a biased electro-optic crystal.
Nano-Prober	Measurement of static device characteristics using fine mechanical probes in vacuum chamber with SEM.

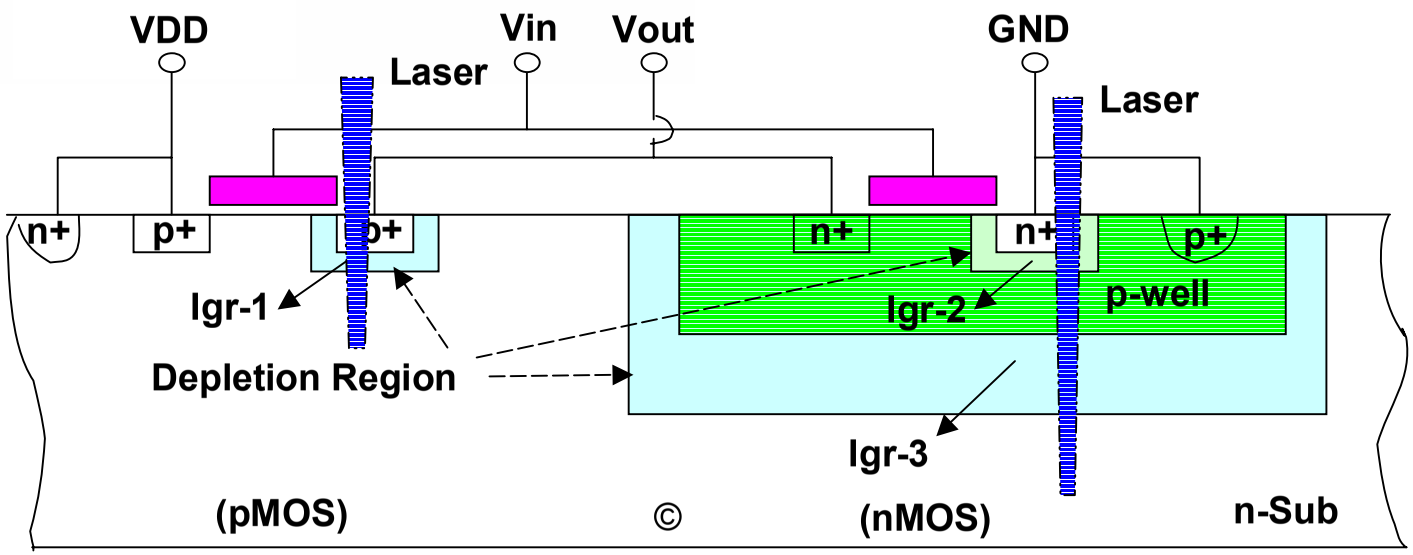
OBIC: Optical Beam Induced Current, EBT: Electron Beam Testing, LVP: Laser Voltage Probing,
TRE: Time Resolved Emission, EOS: Electro-Optic Sampling, SEM: Scanning Electron Microscopy

Node State Observation by OBIC (Optical Beam Induced Current)

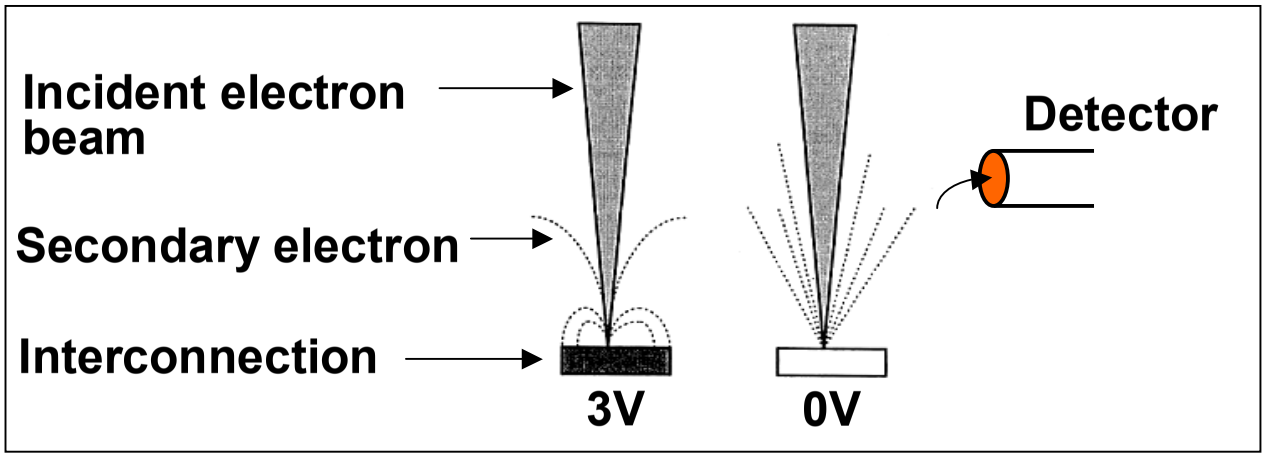


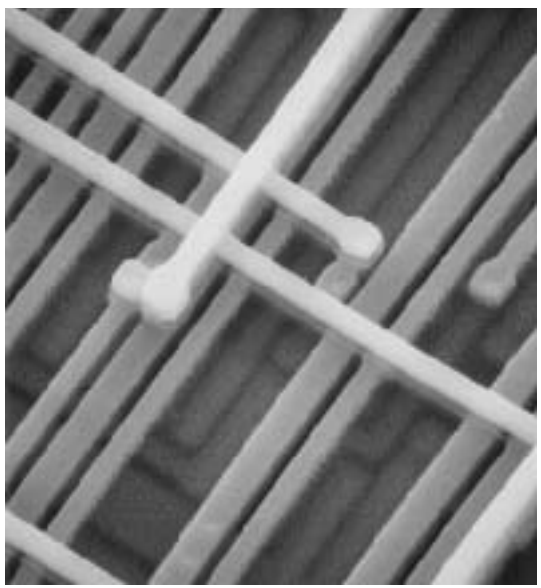




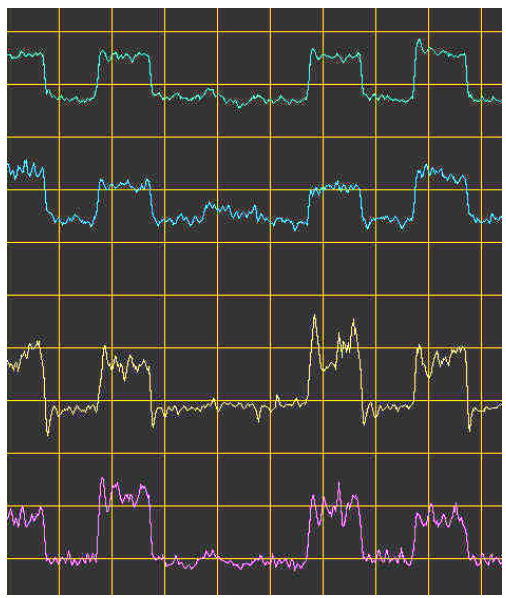


Waveform Measurement by EBT (Electron Beam Testing)



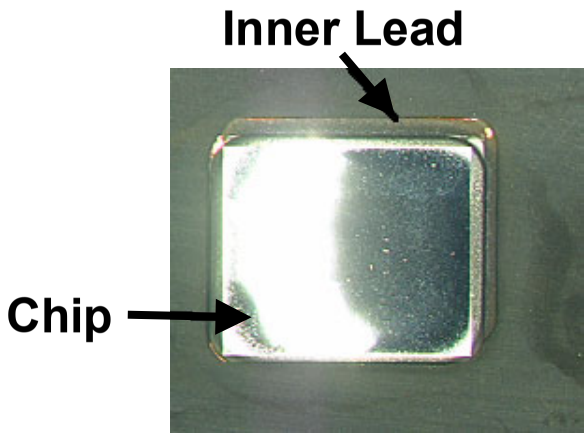


Reactive Ion Etched Surface

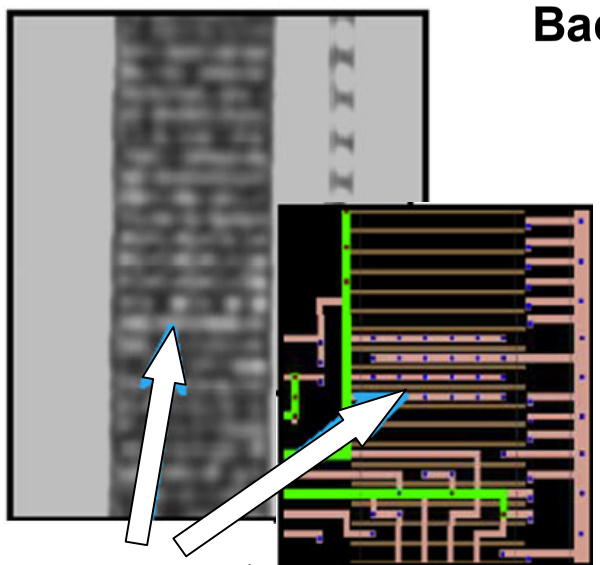


Measured Waveform

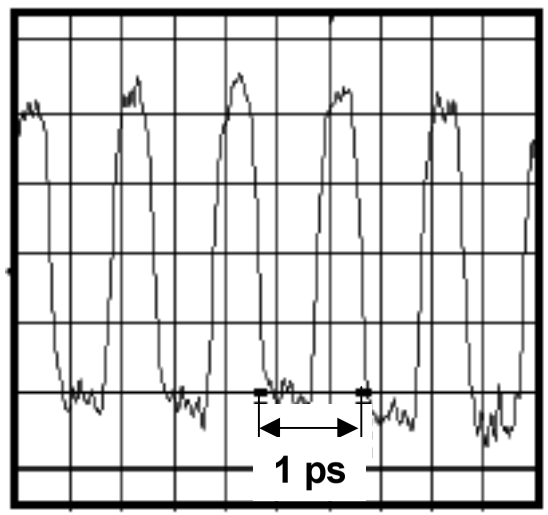
Waveform Measurement from backside by LVP (Laser Voltage Probing)



Backside Polishing

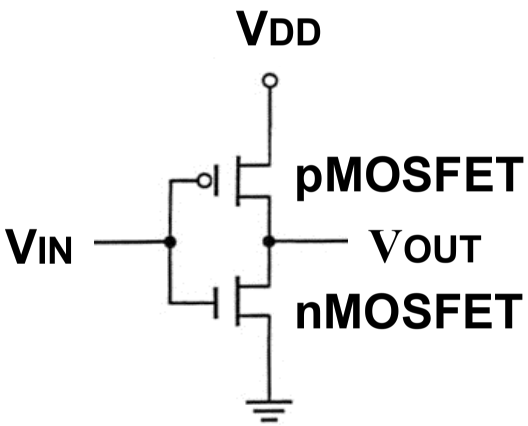


Measurement point

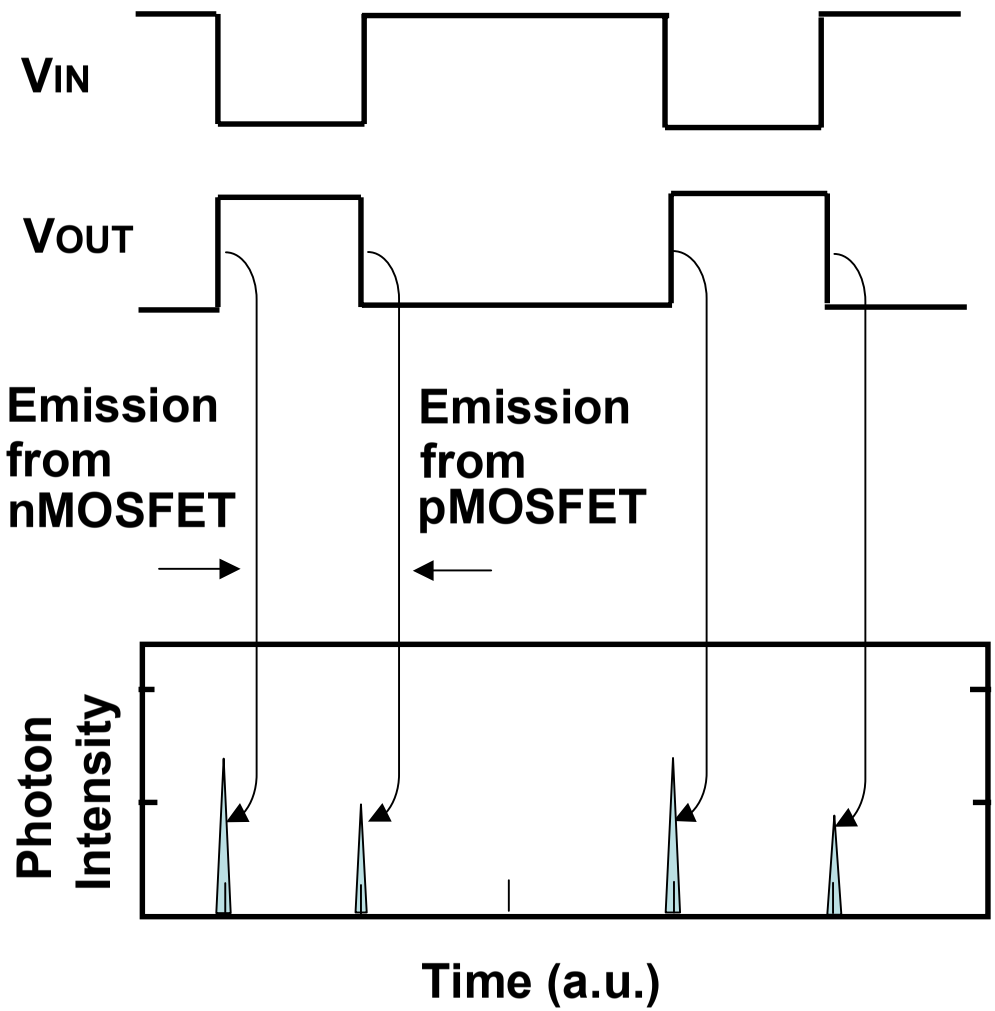


Waveform

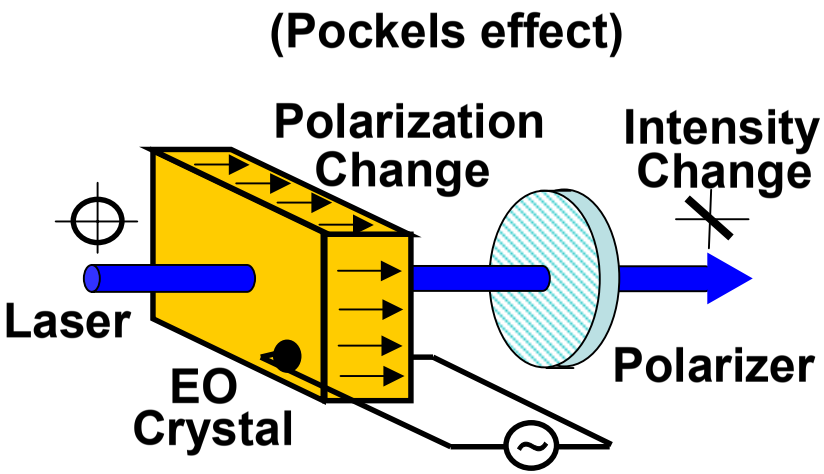
Detection of Photon Emission by TRE (Time Resolved Emission)



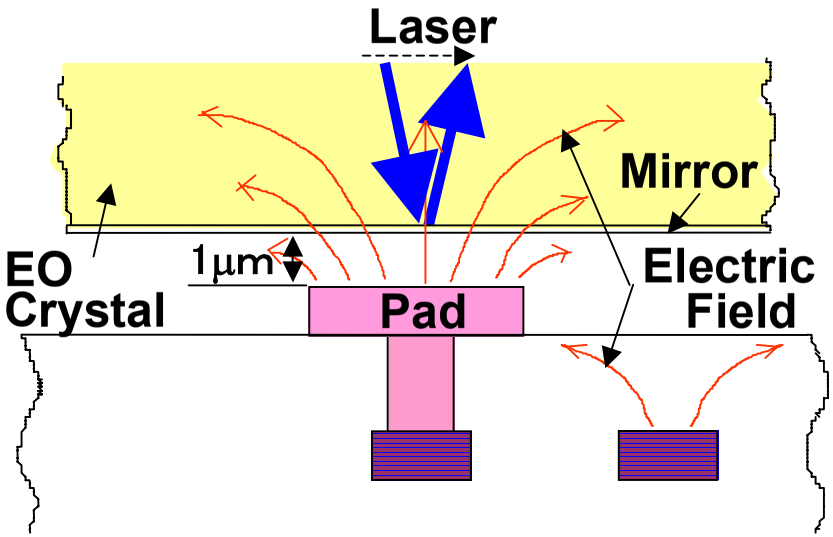
CMOS Inverter

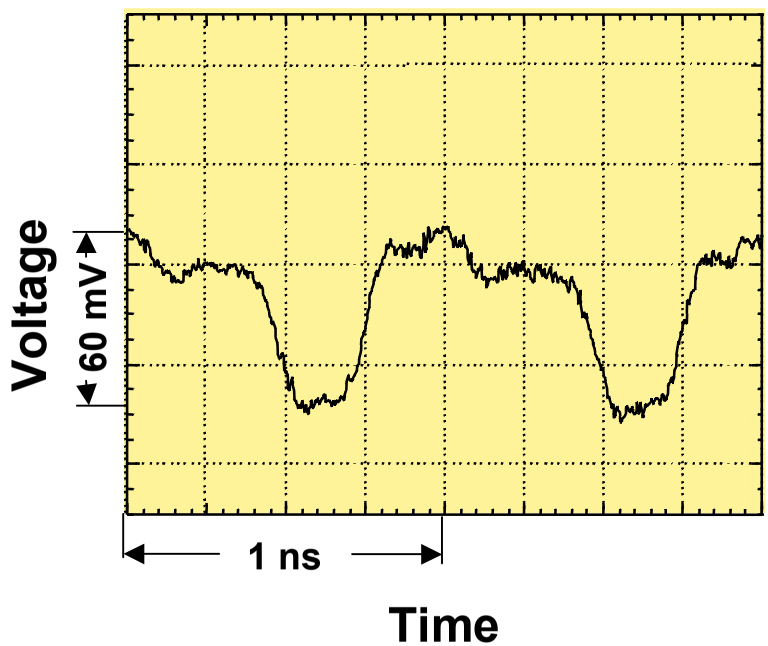


Waveform Measurement by EO-Sampling

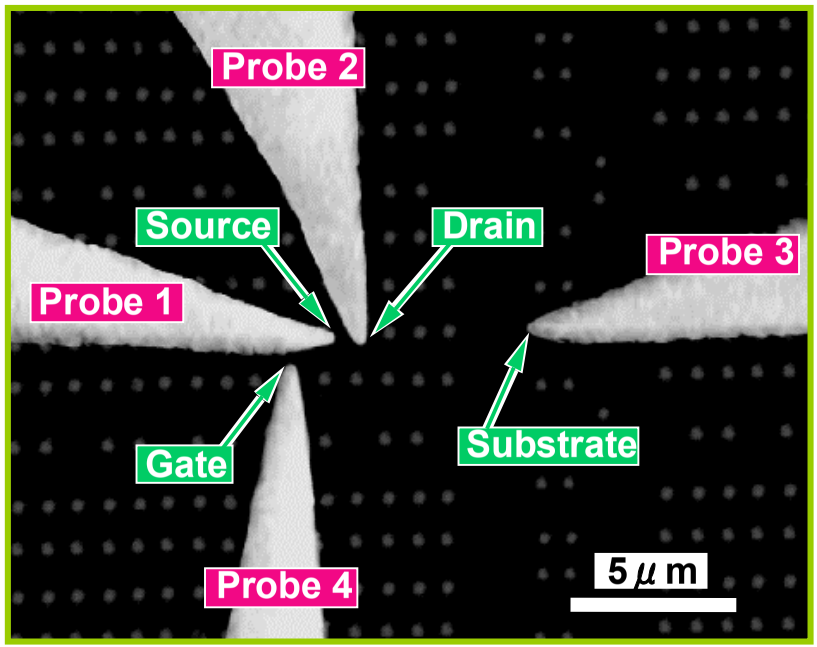


Wide band width : ~ 60 GHz

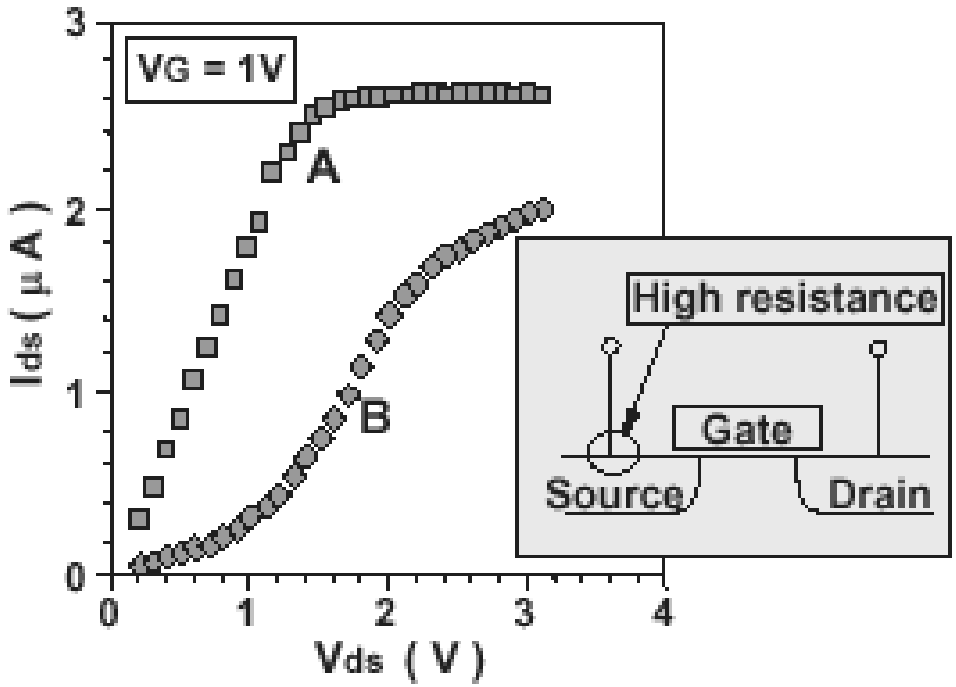




I-V Characteristics Measurement by Nano-prober



Photograph of probes contacting to via plugs



Measured I-V characteristics (A: normal, B: fail)

Tampering Techniques and Related Equipment

Categories of attack	Attack Techniques	Equipment
Chip removal from IC cards	Mechanical sample treatment	Hot plate, Clean bench
Physical Structure Analysis	Cross-sectional analysis Memory cell structure analysis	FIB, SEM, Microscope, Clean bench
Circuit diagram analysis Chip architecture analysis	Interconnection layer lapping with step by step manner	Lapping machine
	Observation of layout patterns	Microscope
	Analysis of circuit diagrams from layout patterns	(Engineers)
	Analysis of chip architecture	
Operational analysis	Packaging of a removed chip Sample preparation Waveform measurement	Wire bonder, NC-Grinder, FIB, EBT, LVP, TRE, EOS
Data reading from ROM and flash memories	Circuit rerouting based on operational circuit analysis	Nano-prober FIB, OBIC, SEM

4. A Case Study of Tampering Sensor Circuits

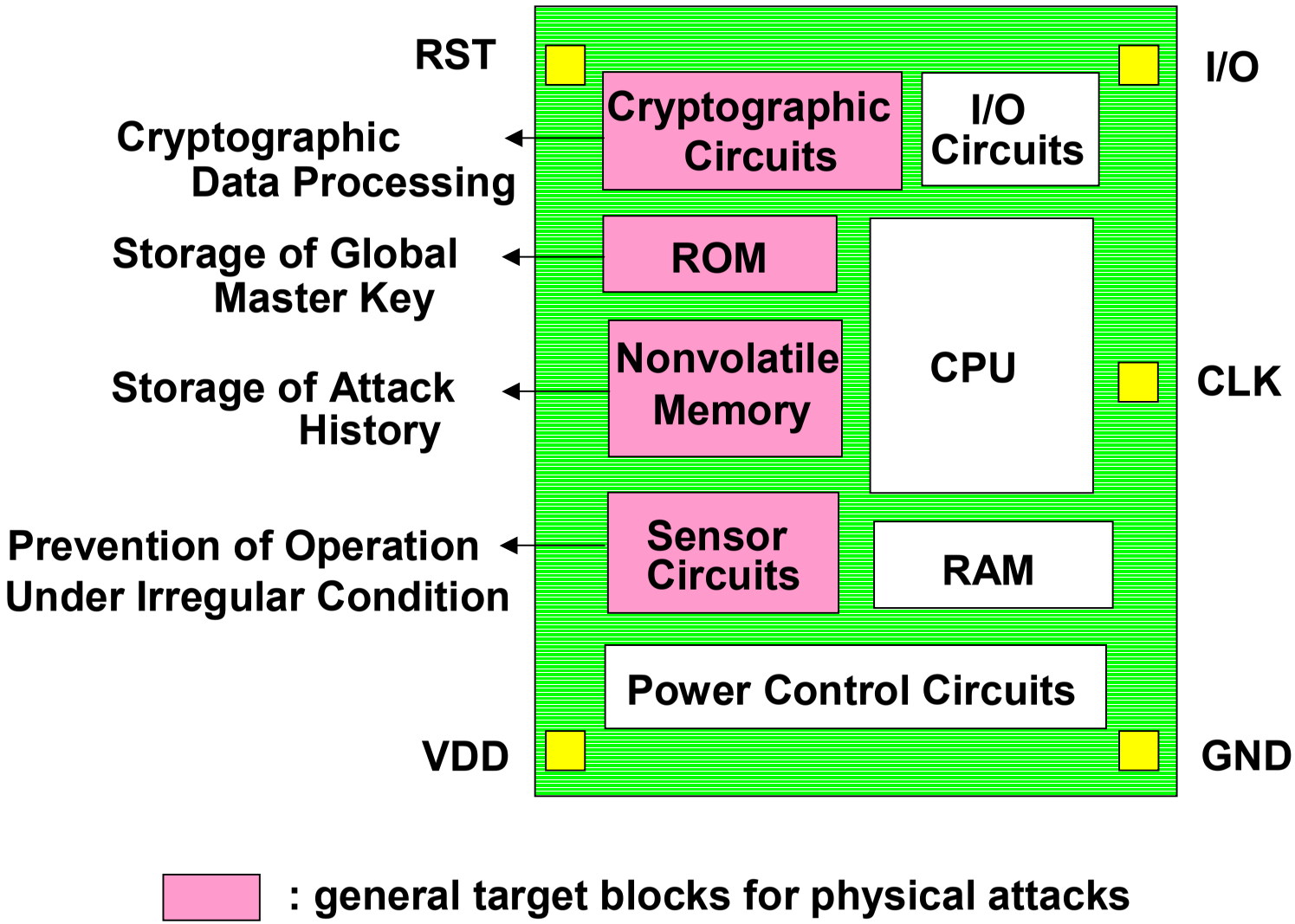
– To describe how failure analysis techniques can be used for tampering IC card chips, we give some results of an experimental physical attack.

– In general, physical attacks may have two objectives:

1. **To read out secret data such as Critical Security Parameters from the chip.**

2. **To alter the function or data for security mechanisms implemented in the chip.**

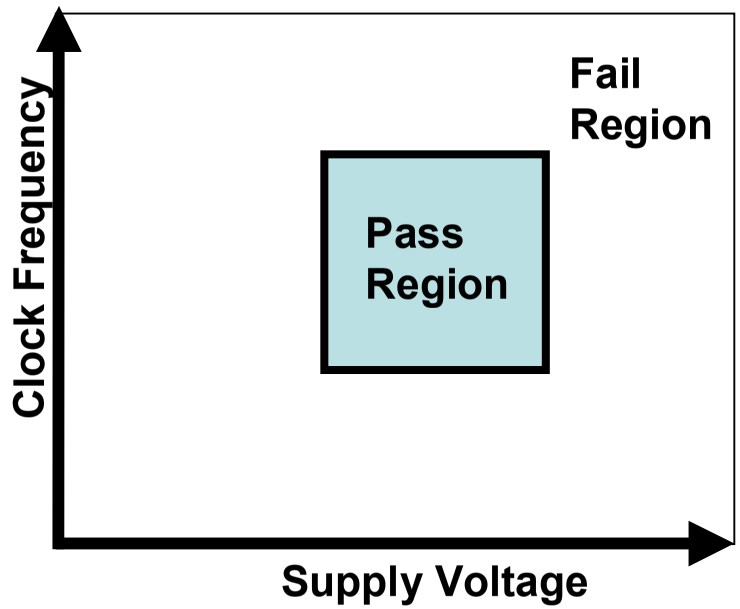
Typical Functional Block Diagram of IC Card Chip



An Observation on a Target Chip

1. The operational range of supply voltage and clock frequency of a target IC card chip was measured.
   It is somewhat narrower than those for conventional LSI chips fabricated with the same pattern rule.

The Shmoo-Plot



2. This fact strongly suggests that the chip is equipped with some sensing circuitry for supply voltage and clock frequency as such a chip often is.

The Assumption

- The target IC card chip contains a user's password.
- An attacker tries to find it, by exhaustive search, namely by inputting every candidate password.
- However, the history of being input wrong password is recorded in EEPROM so that

  the IC card chip may be forced to be inactive

  if the number of attack trials recorded in EEPROM exceeds the initially defined threshold value.

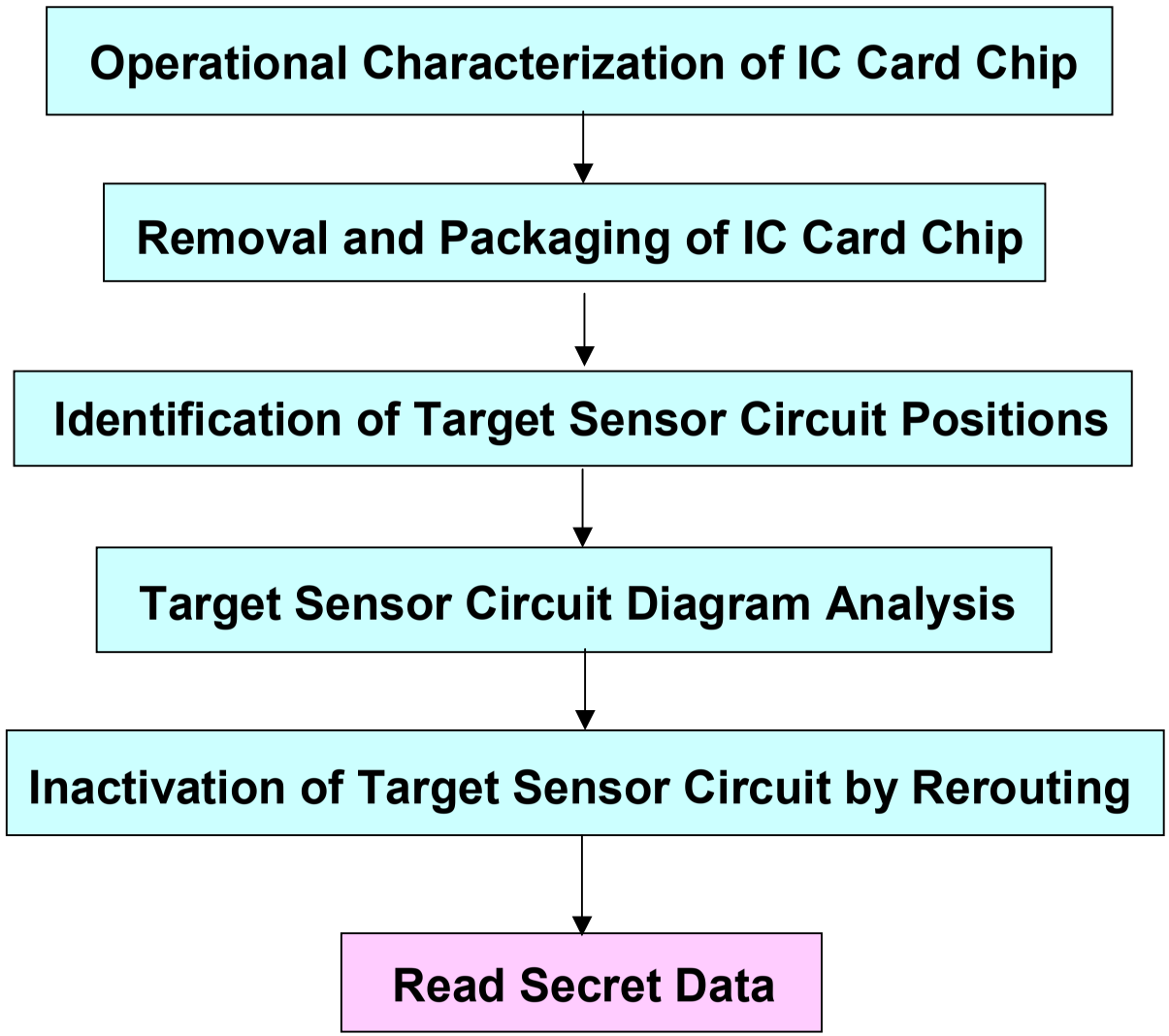
The Attack Scenario

- Thus a promising challenge of the attacker may be destroying the mechanism of writing data into EEPROM.

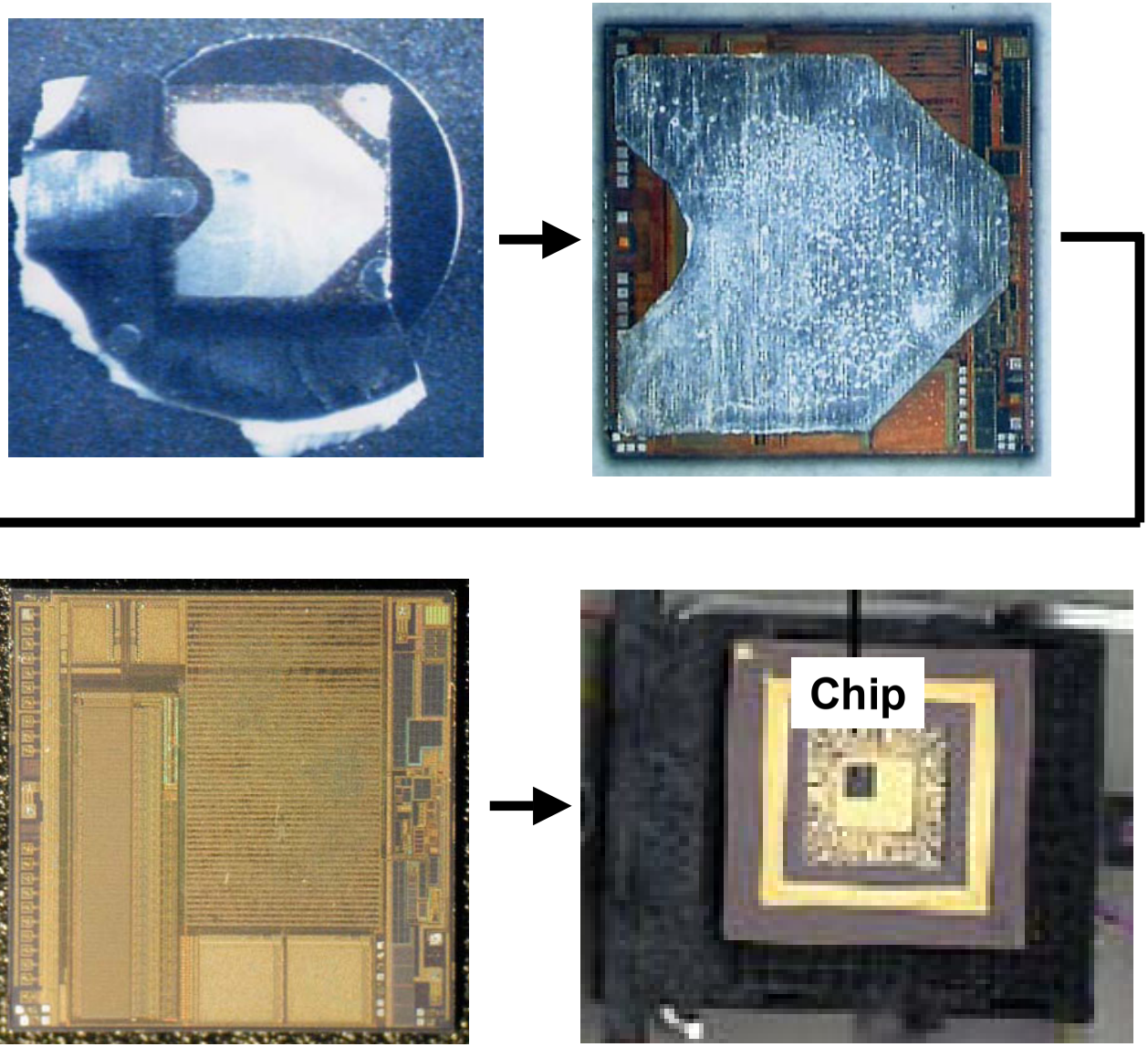
- If the supply voltage may be reduced to low enough, writing data into EEPROM may no longer work and the attacks, such as password exhaustion, cryptanalysis, or software attacks, can be done repeatedly.

- Attacker tries to make the supply voltage sensor circuit inactive.

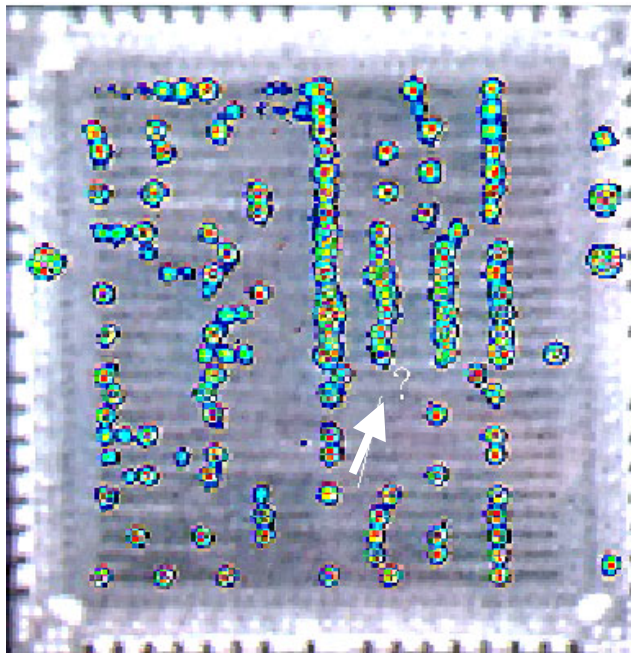
The Flow of Experimental Physical Attack



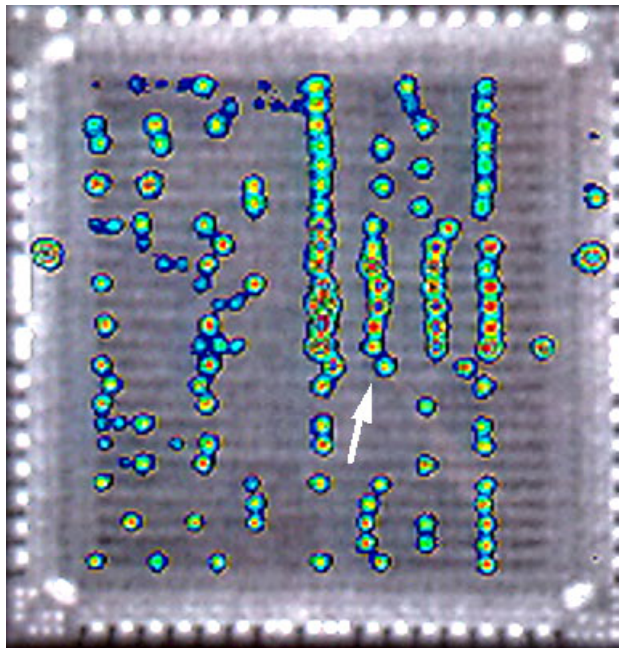
Removal and Packaging of IC Card Chip



Identification of Target Sensor Circuit Positions



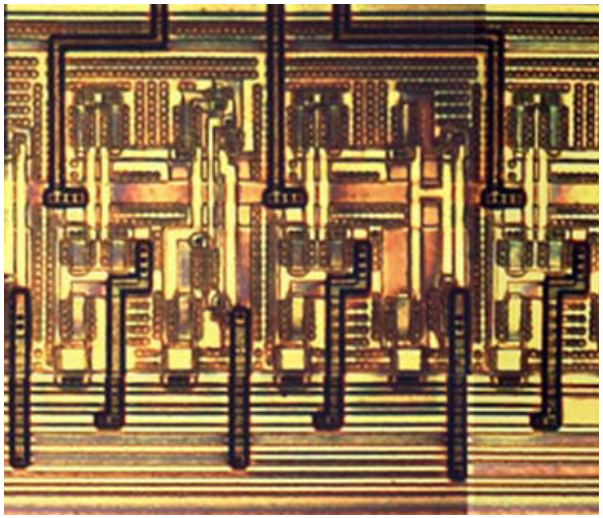
Normal operation condition



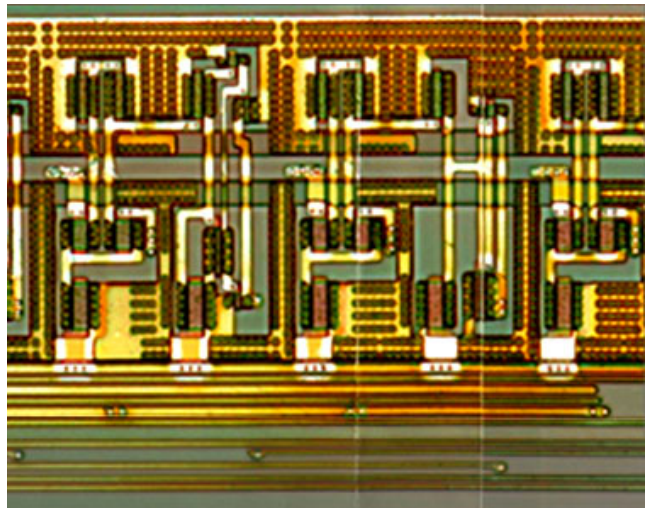
Emission sites increase due to failure. Emission Microscopy is useful to identify sensor circuits.

(To keep the security of the real target chip, the above and next illustrative pictures are the results obtained by experiments on other chips.)

Target Sensor Circuit Diagram Analysis

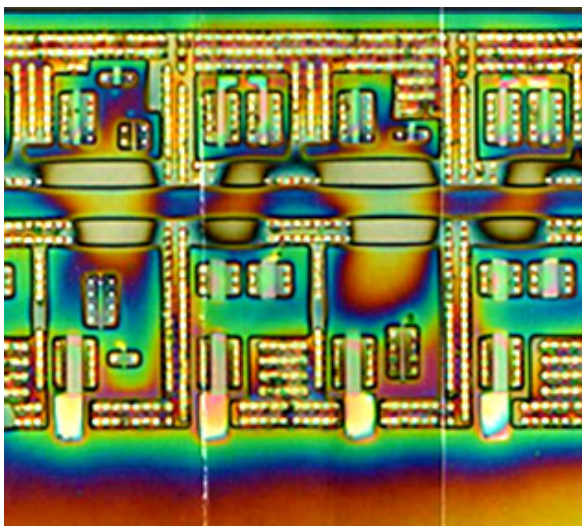


ML2

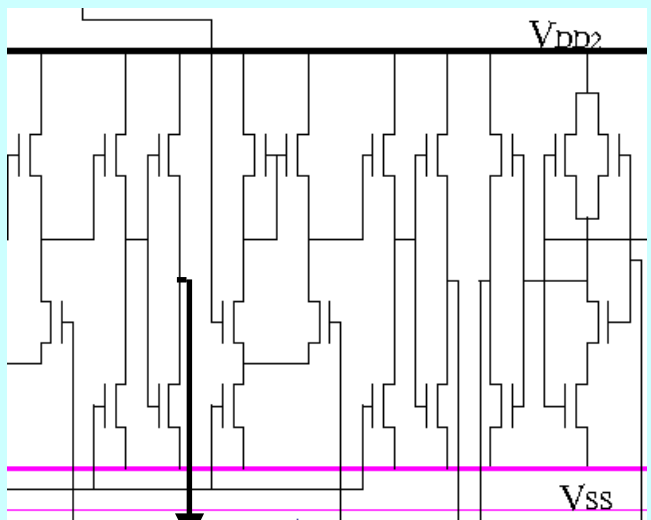


ML1

Observation



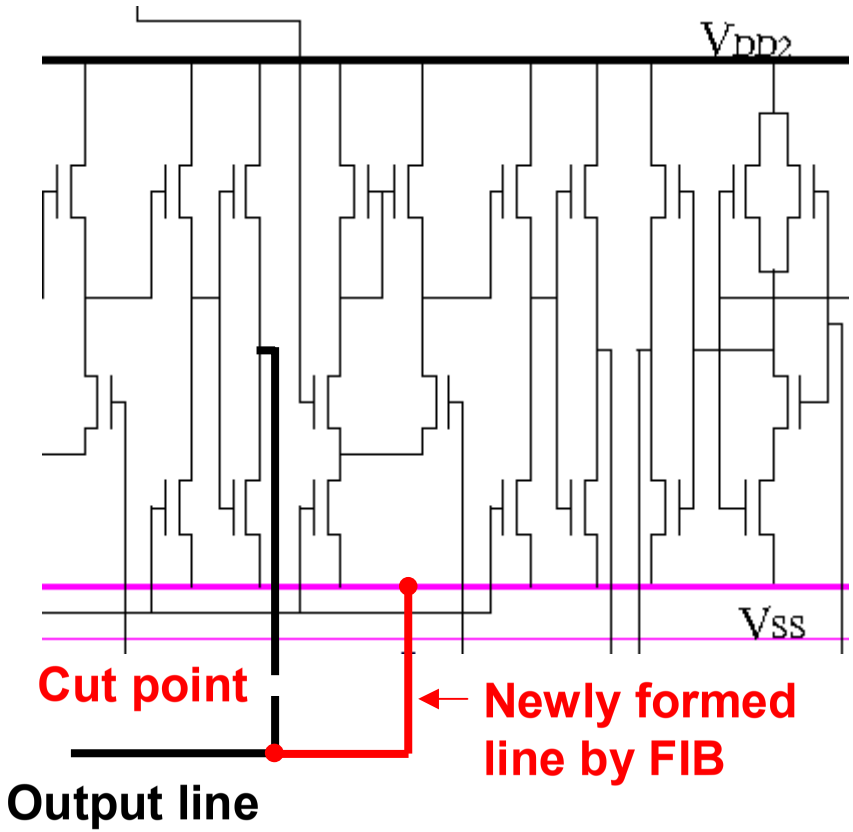
Gate layer

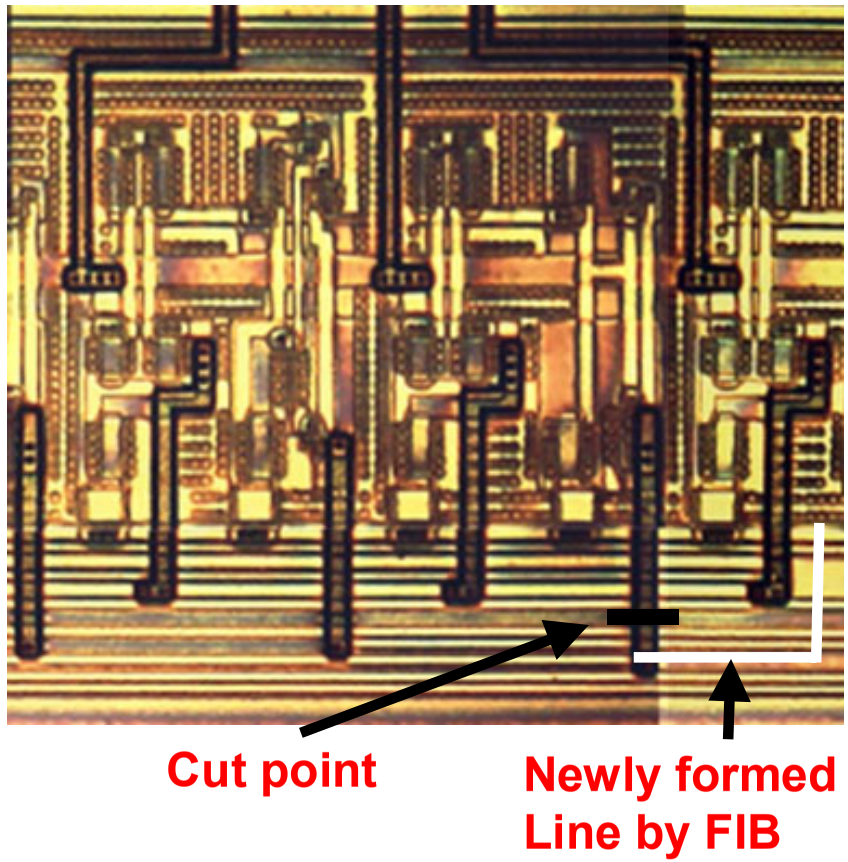


Output

Construction of circuit diagram

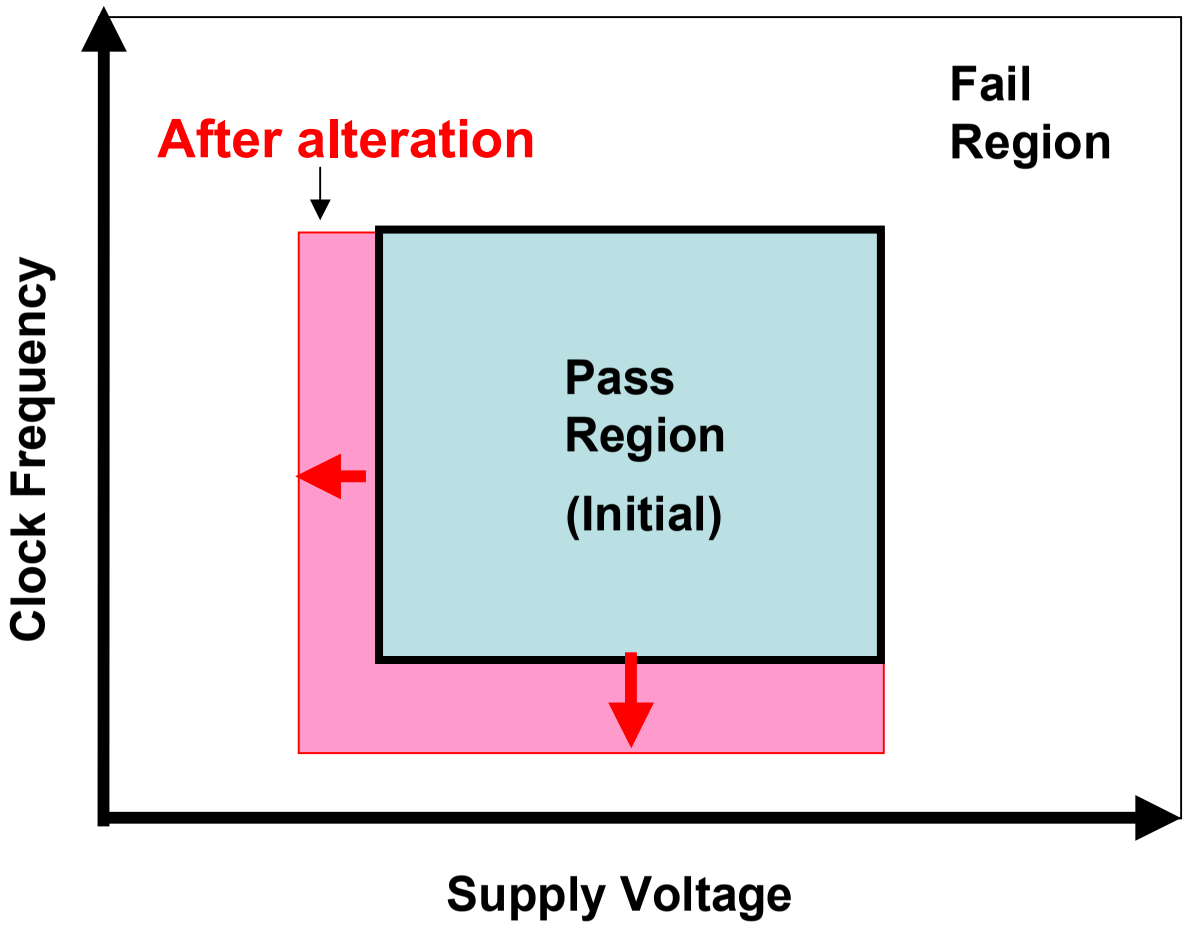
Rerouting to Make Sensor Circuit Inactive



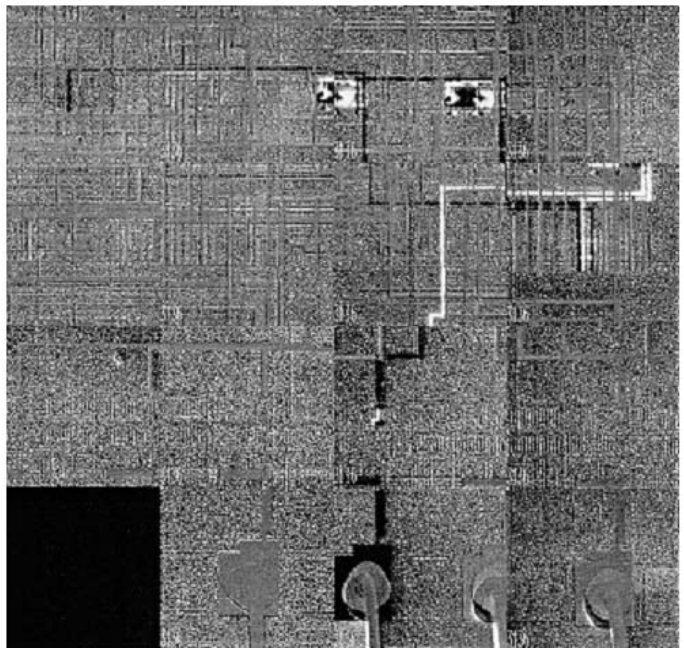


Output line was cut and connected to Vss line.

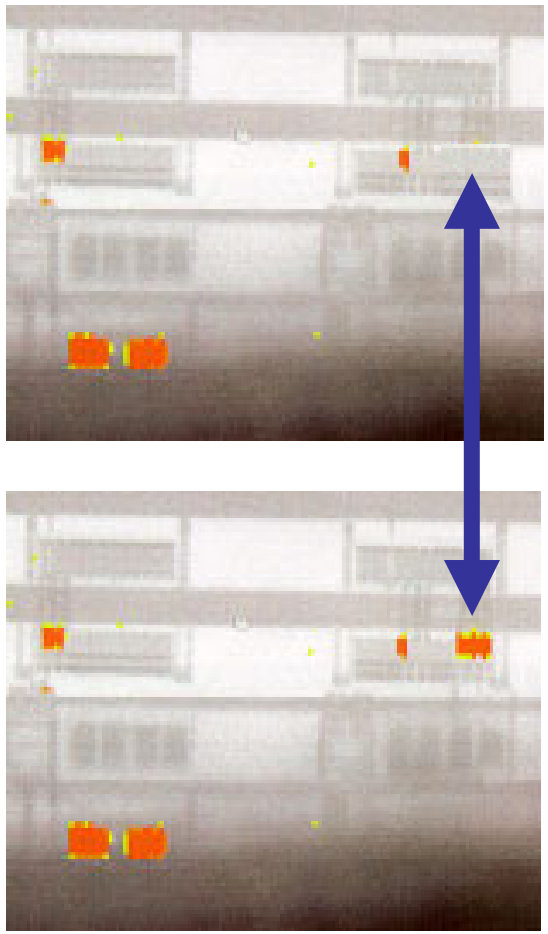
Shmoo-Plot of IC Card Chip Before and After Alteration of Sensor Circuits for Low Supply Voltage and Low Clock Frequency



Superiority the Light Emission Image (LEI) over the Voltage Contrast Image (VCI) of EB Testing

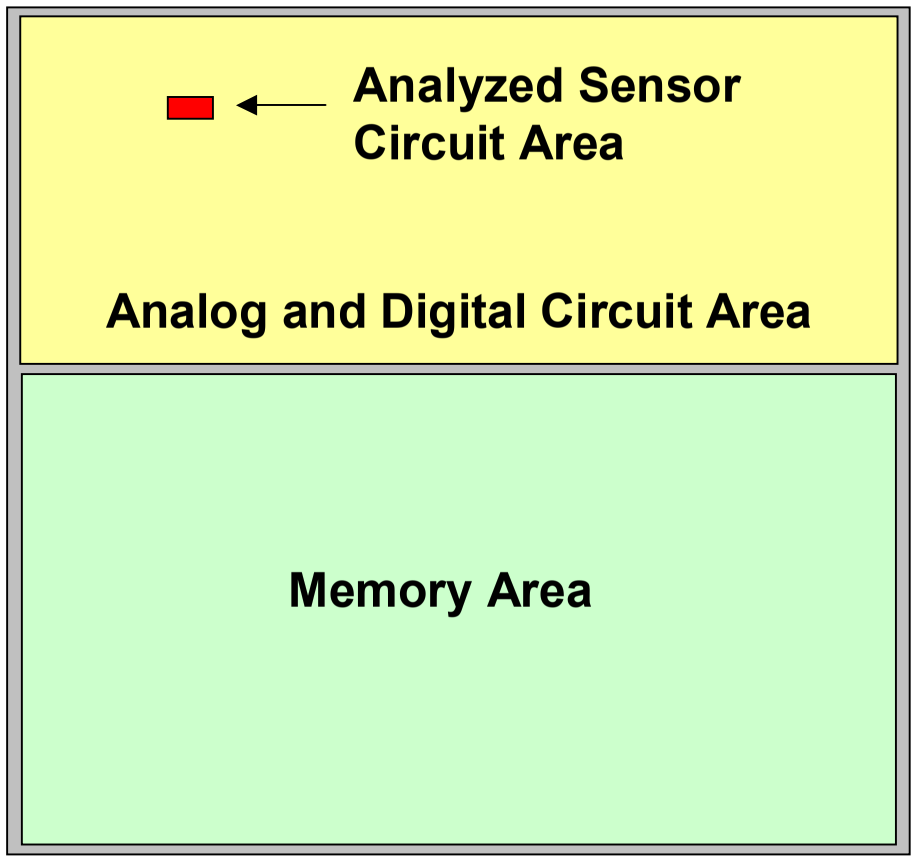


Contrast image difference between operating condition of A and B.
(IFA: Image Fault Analysis)



Emission image difference between operating condition of A and B.

Analyzed Circuits Area is Less Than 2% of the Area of the Chip Excluding the Memory



5. A Tentative Classification of Security Levels

- Based on our experience in failure analysis, we suggest a tentative way of classifying security levels of LSI chips.

- The security levels may be classified by using

  (1) the required skill rank of the attackers or analysts,

  and

  (2) the necessary failure analysis equipment and its cost to attack the chips.

- Our attempt of such a classification is not yet matured and should be improved based on much discussion.

Definition of Skill Ranks

Skill component \ Skill Rank	Expert class	1st class	2nd class	3rd class	4th class	5th class
LSI architecture	α	β	β	γ	—	—
Logic and analog circuit operation	α	α	β	β	γ	γ
Memory circuit operation	α	α	α	β	β	γ
Memory cell structure	α	α	α	β	β	γ
Process technology	α	α	β	γ	—	—
Failure analysis technology	α	α	α	β	β	γ
Measurement technology	α	α	α	β	γ	—
Experience (minimum years)	15	13	10	8	5	3

α : expert, β : proficient, γ : sufficient $\quad \alpha > \beta > \gamma$

Tentative Candidate of Five Security Levels of LSI Chips Based on Failure Analysis Equipment and Skills of Analyst

Security level	Necessary FA equipment	Equipment total cost [M$]	Skill rank
Beyond	Unknown (today)	?	?
A (+2)	EOS TRE Nano-prober	10+6	Expert
B (+1)	LEM/MCT LVP OBIC Reverse engineering software	6.5+3.5	1st
C (0)	LEM/CCD SEM FIB Lapping Machine EBT	2.5+4	2nd
D (-1)	Electrical measurement system	0.5+2	3rd
E (-2)	Hot-plate Clean bench Wire-bonder	0.5	4th, 5th

Current average failure analysis capability may correspond to "level C".

"Beyond" means the level non-attackable by today's FA technologies.

6. Summary

- We have described relationships between LSI tamper resistance and FA techniques.
- Tamper resistance of LSI chips against physical attacks should be evaluated or tested on the basis of latest technologies.
- To facilitate an understanding of the level of today's failure analysis techniques we have demonstrated an inactivation of sensor circuits where emission microscopy plays an important roll.
- Then we have given a tentative way of classifying the security levels for LSI chips with respect to the required equipment and the required skills of attackers.

References

[1] S. Nakajima and T. Takeda, "Failure analysis in halfmicron and quartermicron eras, " Proceeding of the 6th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF 95), pp. 273-280, 1995.

[2] S. Nakajima, T. Ueki, Y. Shionoya, K. Mafune, N. Kuji, S. Nakamura, Y. Komine and T. Takeda, "Current status of failure analysis for ULSIs, " Microelectronics Reliability, Vol. 38, pp. 1369-1377, 1998.

[3] S. Nakajima, S. Nakamura, K. Kuji, T. Ueki, T. Ajioka and T. Sakai, "Construction of a cost-effective failure analysis service network --- Microelectronic failure analysis service in Japan," Microelectronics Reliability, Vol. 42, pp.511-521, 2002.

[4] Y. Mitsui, et al, "Physical and chemical analytical instrument for failure analyses in G-Bit devices, " Technical Digest of International Electron Devices Meeting, pp.329-332, 1998.

[5] C. Hashimoto, T. Takizawa, S. Nakajima, M. Shinagawa and T. Nagatsuma, "Observation of the internal waveforms in high-speed high-density LSIs using an EOS prober, " Microelectronics Reliability, Vol. 41, pp. 1203-1209, 2001.

[6] M. K. Mc Manus, J. A. Kash, S. E. Steen, S. Polonsky, J. C. Tsang, D. R. Knebel and W. Huott, "PICA: Backside failure analysis of CMOS circuits using Picosecond Imaging Circuit Analysis," Microelectronics Reliability, Vol. 40, pp. 1353-1358, 2000.

[7] A. Tosi, F. Stellari, F. Zappa and S. Cova, "Backside Flip-Chip testing by means of high-bandwidth luminescence detection," Microelectronics Reliability, Vol. 43, pp. 1669-1674, 2003.