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

Tsutomu Matsumoto [1] **Shigeru Nakajima** [2] **Tadashi Shibata** [3] **Atsuhiro Yamagishi** [4]

[1] Yokohama National University, Graduate School of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan, Email: tsutomu@mlab.jks.ynu.ac.jp

[2] Van Partners Corporation
1-4-6 Nezu, Bunkyo-ku, Tokyo 113-0031, Japan, Email: nakajima@van-partners.com

[3] University of Tokyo, School of Frontier Sciences
5-1-5 Kashiwanoha, Kashiwa-shi, Chiba 277-8561, Japan, Email: shibata@ee.t.u-tokyo.ac.jp

[4] Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan, Email: a-yamagi@ipa.go.jp

Abstract: *Tamper resistance of LSI chips against physical attacks is studied from the viewpoint of LSI failure analysis. 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. We give some results from our case study on inactivation of sensor circuits where emission microscopy plays an important roll. 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.*

Keywords: tampering, tamper resistance, failure analysis, physical security testing

I. Introduction

The information security technologies including cryptography are increasing their importance. In particular, the security of cryptographic hardware embedded in LSI chips is attracting keen attention of users and systems providers, because such chips are often delivered to and used by the general public in the form of contact or wireless IC cards or embedded Trusted Platform Modules, etc. Since many of the failure analysis (FA) techniques are applicable to tampering cryptographic hardware, it is worthy to consider tamper resistance of LSI chips from the viewpoint of the latest techniques for LSI failure analysts. In this paper, after describing the principles and outline of FA techniques, we exemplify that such FA techniques, particularly, emission microscopy and other advanced techniques are really useful, by introducing an experimental case study of making sensor circuits inactive so that an analyst can conduct logical attacks including an exhaustive search for a secret key or password hidden in a target chip. Finally, based on our experience, we describe a tentative way to classify the security levels for LSI chips with respect to the required FA equipment and the required skills of analysts or attackers.

II. Basic Physical Phenomena in LSI Chips

The basic physical phenomena in LSI chips can be categorized into two classes; generated and stimulated physical phenomena. Generated physical phenomena are those generated in operating LSI chips and have three types as shown in Fig.1 for MOSFETs and bipolar transistors. 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.

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, as shown in Fig. 2.

Typical methods to detect these physical phenomena include voltage measurement by non-contact or contact probing,

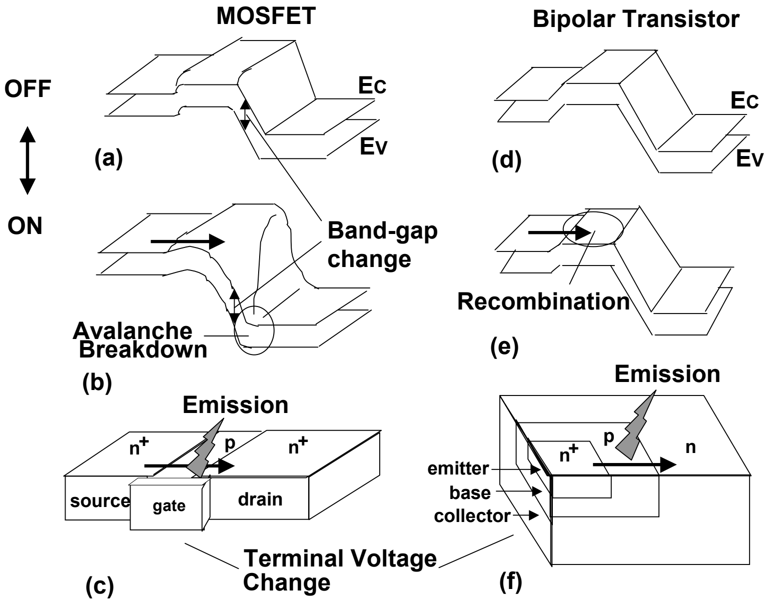


Fig.1 Physical phenomena generated in operating MOSFETs and bipolar transistors.

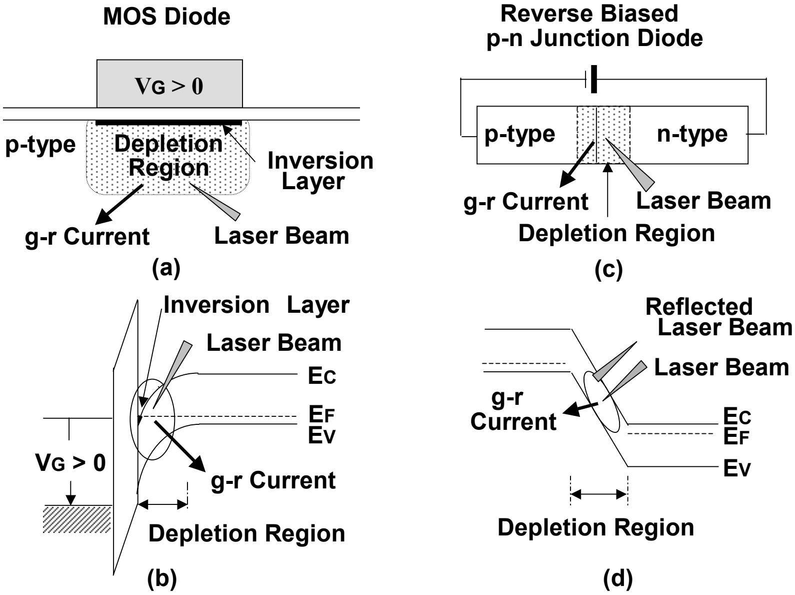


Fig.2 Generation-recombination current flow in depletion region by laser beam irradiation. Polarization of reflected laser beam is varied with electric field strength in operating device due to Frantz-Keldish effect.

Table 1. Measurement methods of electrical characteristics of LSI

Method	Features
OBIC: Optical Beam Induced Current	Measurement of "H" or "L" state of nodes by detecting substrate current generated by laser beam exposure.
EBT: Electron Beam Testing	Waveform measurement by detecting amount of secondary electrons emitted from operating interconnections.
LVP: Laser Voltage Probing	Waveform measurement by detecting intensity of laser beam reflected at reverse biased p-n junction in devices.
TRE: Time Resolved Emission	Waveform measurement by detecting intensity of photon emission from operating devices.
EOS: Electro-Optic Sampling	Waveform measurement by detecting polarization of laser beams after pass-through a biased electro-optic crystal.
Nano-Prober	Measurement of static device characteristics using fine mechanical probes in vacuum chamber with Scanning Electron Microscopy (SEM).

photon detection from front-side or backside of the chip, and, detection of polarization change of laser beam reflected at the depletion region, as shown in Fig. 3. Note that silicon crystal with low impurity concentration is transparent for the light if its wavelength is longer than 1.1 μm.

III. Failure Analysis Techniques

This section describes typical FA techniques [1][2][3].

Sample preparation is very important for successful FA. Typical sample preparation techniques are summarized in Fig. 4 and Fig. 5. Cross-section formation by focused ion beam (FIB) etching and revealing an interconnection layer by lapping are used as sample preparation techniques for vertical structure analysis and layout pattern observation. Non-destructive sample preparation techniques, such as probing pads formation by FIB, revealing interconnection layers by reactive ion etching (RIE), backside grinding to reduce the chip thickness and formation of silicon immersion lens on backside are used to sample preparation for measurement of electrical characteristics of chips.

We summarize typical methods of measuring electrical characteristics in Table 1. Method of the Optical Beam Induced Current (OBIC) is useful to examine "High" or "Low" state of nodes because depletion region width is dependent upon reverse bias voltage of p-n junction and optical beam induced current (gr-current generated by laser beam irradiation) is dependent upon depletion region width. Fig. 6 shows results of OBIC analysis for an inverter circuit. Voltage of diffused areas with dark OBIC image is low. The OBIC image of diffused areas in nMOSFETs, which are formed in a p-well, is always bright. The reason of this result is that the gr-current generated in wide depletion region of p-n junction between well and substrate is much larger than the optical beam induced current generated in drain junction of nMOSFETs.

Fig. 7 shows examples of electron beam testing (EBT) results. For reliable EBT, it is desirable to expose the interconnection surface or to form probing pads.

Fig. 8 shows the Laser Voltage Probing (LVP) method. Laser beam is irradiated to a specific device area and reflected laser beam is detected after passing through a polarizer. Amount of polarization of reflected laser beam is changed due to band-gap variation in depletion region with operation voltage.

Fig. 9 shows the Time Resolved Emission (TRE) method. The nMOSFET and pMOSFET in a CMOS inverter emit photons at rise and down cycles, respectively. Emitted photons are detected with high time resolution from the backside. Fig. 10 shows the principle of Electro-Optic Sampling (EOS) method [4]. Polarization of laser beam is changed after pass through the electro-optic crystal under influence of electric field. Amount of changed polarization angle is dependent on strength of electric field in the EO-crystal (Pokels effect). Since response time of EO-crystal's polarization characteristics to electric field variation is very short, band width of EOS method is more than 60 GHz. DC characteristics of any device in an LSI is measurable by using a nano–prober, as shown in Fig. 11 [5].

As illustrated above, the failure analysis techniques may be used as very powerful tampering techniques, or the tools to evaluate or test the level of tamper resistance that a particular LSI does provides. We summarize the relationship in Table 2.

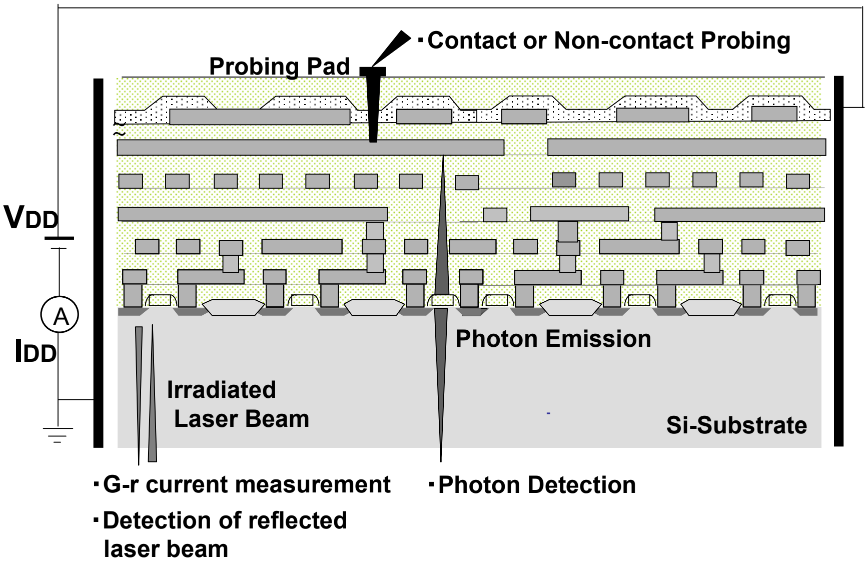


Fig.3 Typical methods to detect physical phenomena in LSIs.

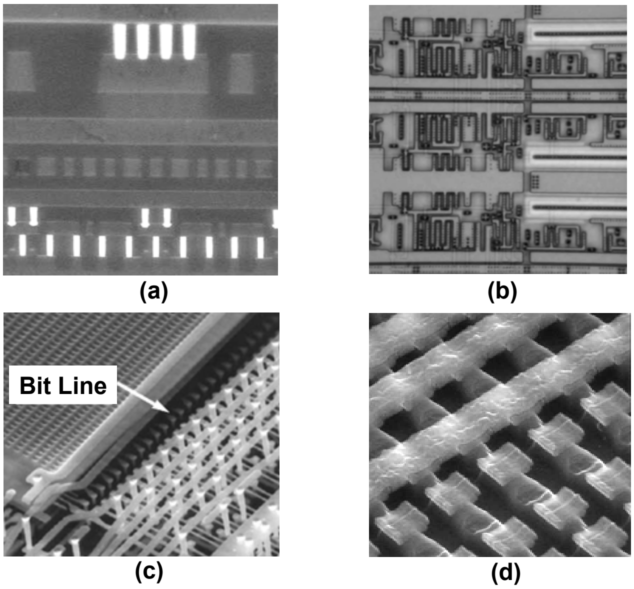


Fig. 4 Sample preparation techniques for structural analysis of LSIs: (a) cross-section formation by FIB, (b) successive metal layer lapping, (c) & (d) interlayer dielectric film removal by wet etching.

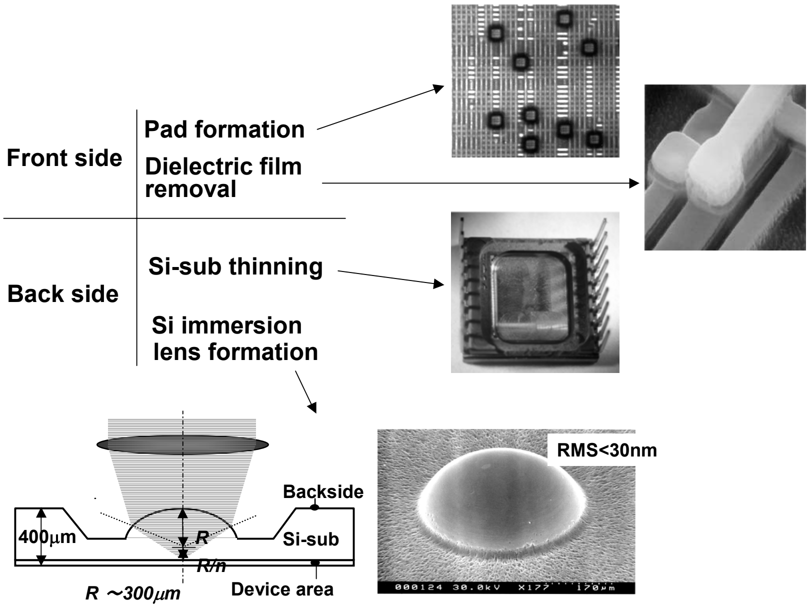


Fig. 5 Sample preparation techniques for operating waveform measurements.

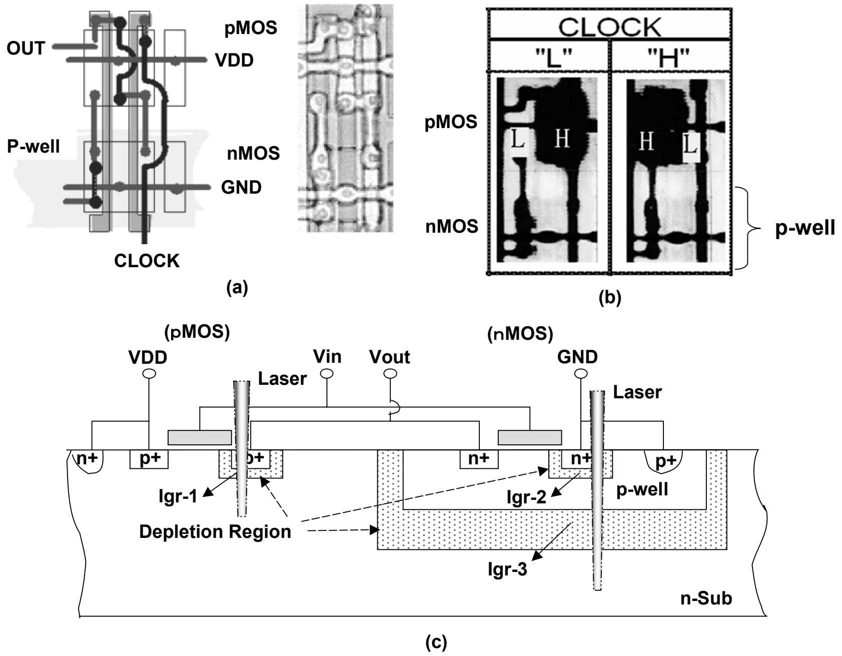


Fig. 6 Observation of "H" or "L" state of node by OBIC.

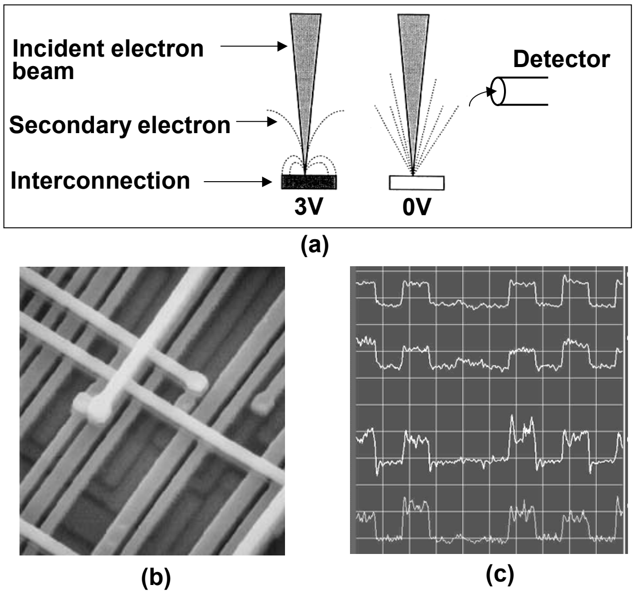


Fig. 7 Measurement of waveforms from front-side by EBT.

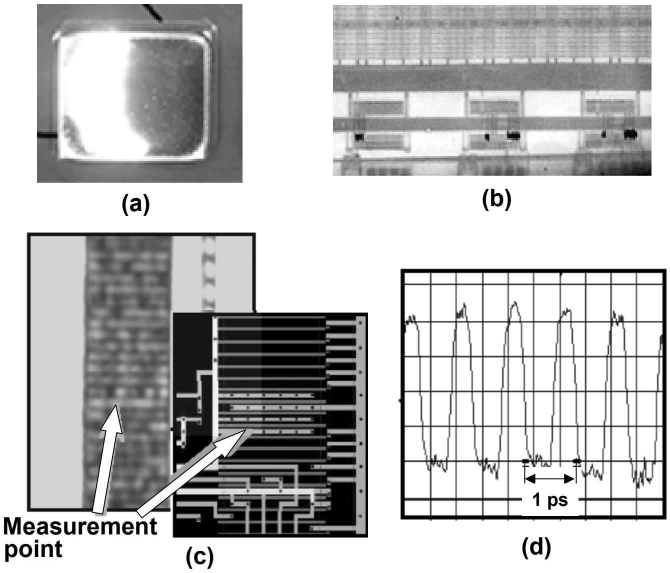


Fig. 8 Measurement of waveform from backside by LVP.

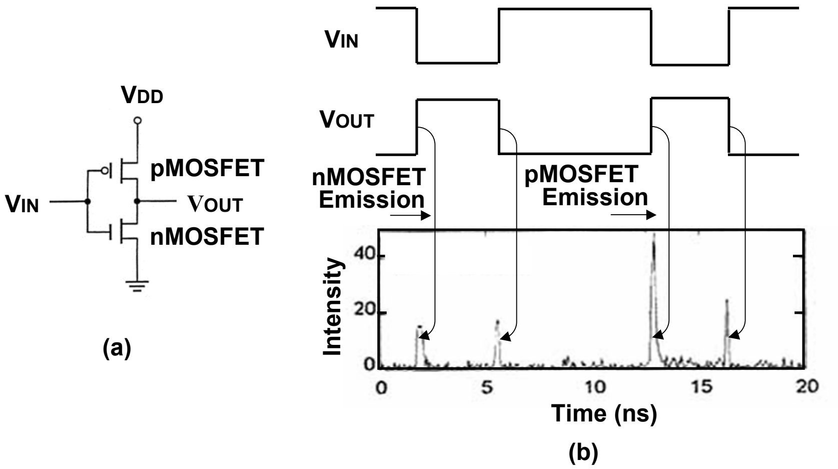


Fig. 9 Measurement of photon emission from backside: (a) circuit diagram of CMOS inverter and (b) detected time resolved photon emission from CMOS inverter by TRE.

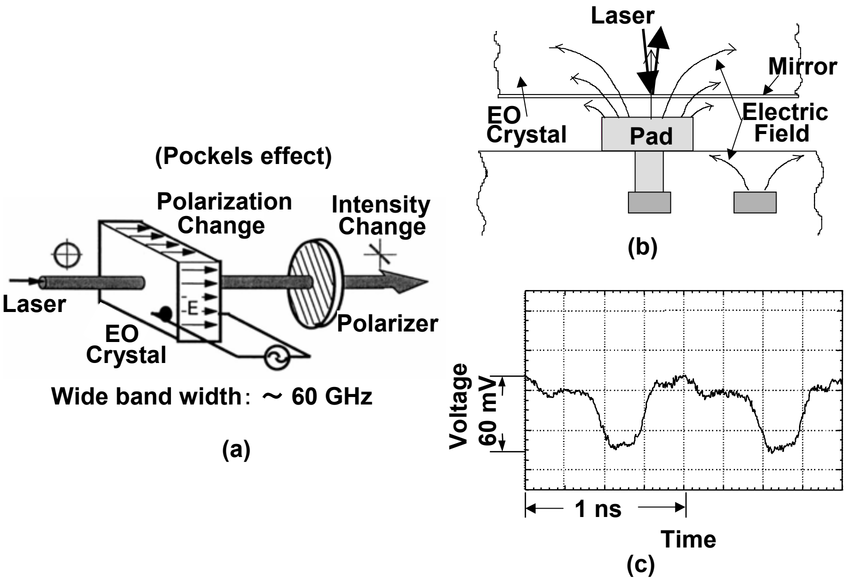


Fig. 10 Principle of EO-sampling and result of high speed and low Voltage signal measurement.

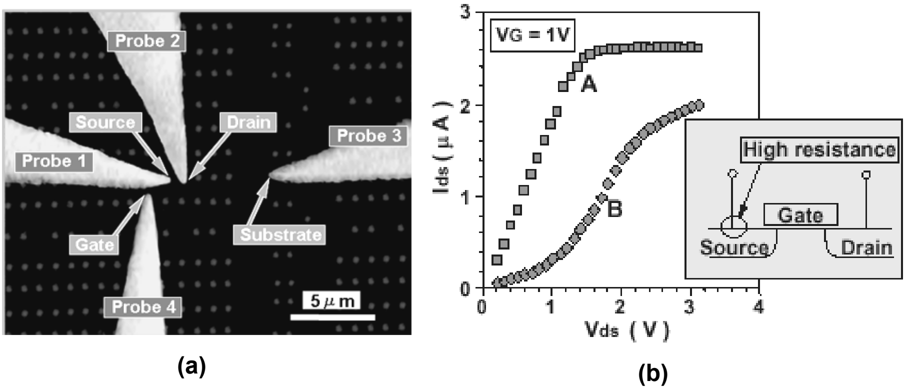


Fig. 11 Measurement of DC characteristics of a MOSFET in a sRAM cell by using a nano-prober: (a) photograph of probes contacting to via plugs, (b) Measured I-V characteristics (A:normal, B:abnormal).

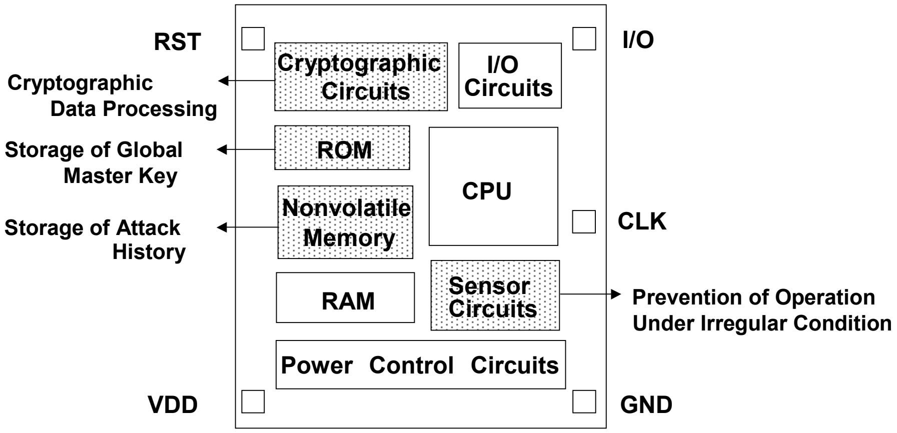


Fig. 12 Basic block diagram of IC card Chip with general target blocks for physical attacks shown as dotted blocks.

Table 2. 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	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 Analysis of chip architecture	(Engineers)
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

IV. A Case Study of Tampering Sensor Circuits

In this section, we describe how failure analysis techniques can be used for tampering IC card chips. Then 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.

For example, as shown in Fig. 12, the targets of physical attacks may be the circuit blocks that are related to secret data storage, cryptographic data processing, and sensor circuits for protecting IC card chips from abnormal operating conditions.

To conduct an experimental attack, we obtained IC card chips and reader/writers. Then we measured the Shmoo-plot, namely the region of operating conditions described by supply voltage and clock frequency, of the chips. The region of pass condition is somewhat narrower than that for usual chips fabricated with the same pattern rule. 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.

We assume the following scenario. The IC card chip contains a user's password and 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.

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.

Based on the above observation, we decided to adopt the attack flow depicted as Fig. 13. The IC card chip is removed from IC card and it is packaged as shown in Fig. 14 and Fig. 15, respectively. Then, to identify the position of sensor circuits, the emission microscopy is utilized, because the specific emission sites relating to the sensor circuits vary according to the pass and the fail operational conditions.

After identifying the sensor circuit positions, sensor circuit diagrams are analyzed by revealing interconnection layers with layer after layer, as shown in Fig. 16. Then, the output interconnection line of the sensor circuit for low supply voltage is rerouted to make it to be inactive for low supply voltage.

At the sensor circuit identified by the emission microscopy, voltage contrast image of it's output line was different for pass and fail conditions. Therefore, we confirmed the effectiveness of emission microscopy to identify sensor circuit positions with short time, because emission sites can be found by global observation of the chip. The analyzed circuit area for low supply voltage and low clock frequency was less than the 2% of the whole chip area without memory area.

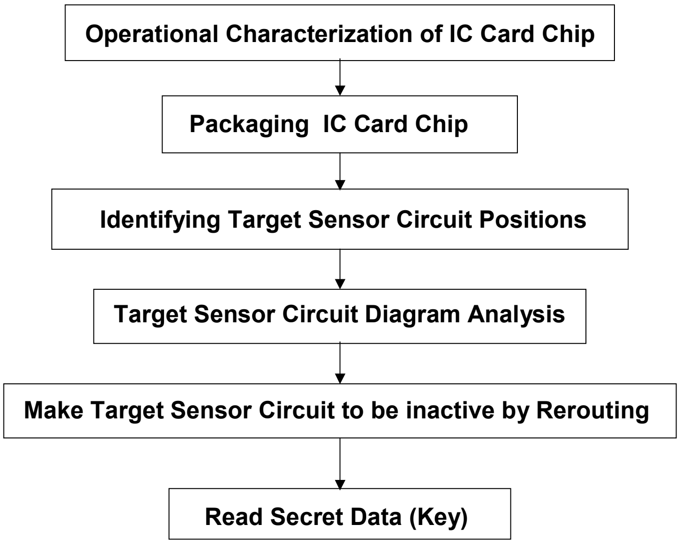
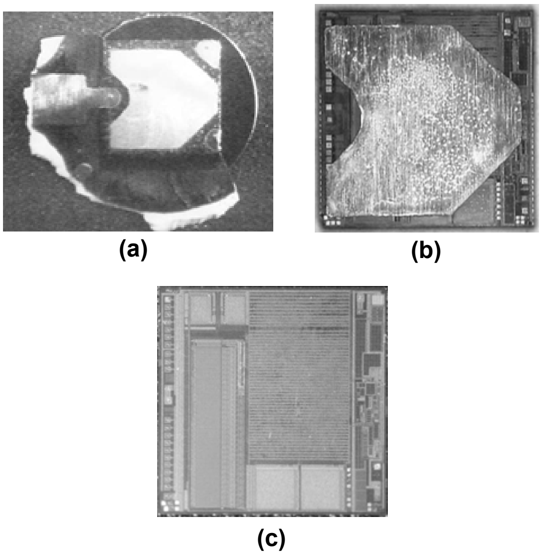

Operational Characterization of IC Card Chip
Packaging IC Card Chip
Identifying Target Sensor Circuit Positions
Target Sensor Circuit Diagram Analysis
Make Target Sensor Circuit to be inactive by Rerouting
Read Secret Data (Key)

Fig. 13 A Flow of Physical Attack


(a)

(b)

(c)

Fig. 14 Flow of chip removal from IC card ((a) to (c)).

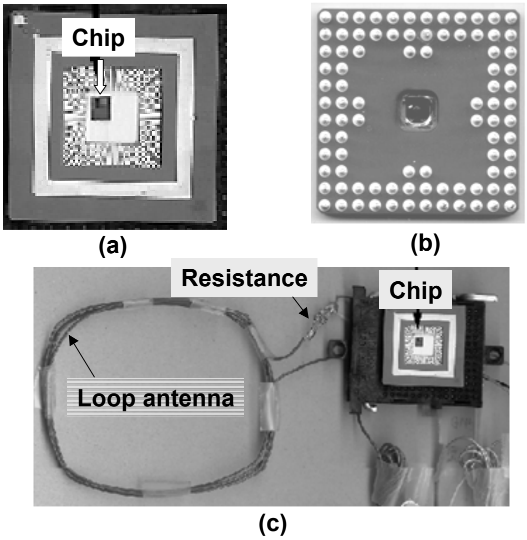


Fig. 15 Packaged removed chip and build-up spurious IC card with loop antenna connected to package. The spurious IC card operates as well as real non-contact IC card.

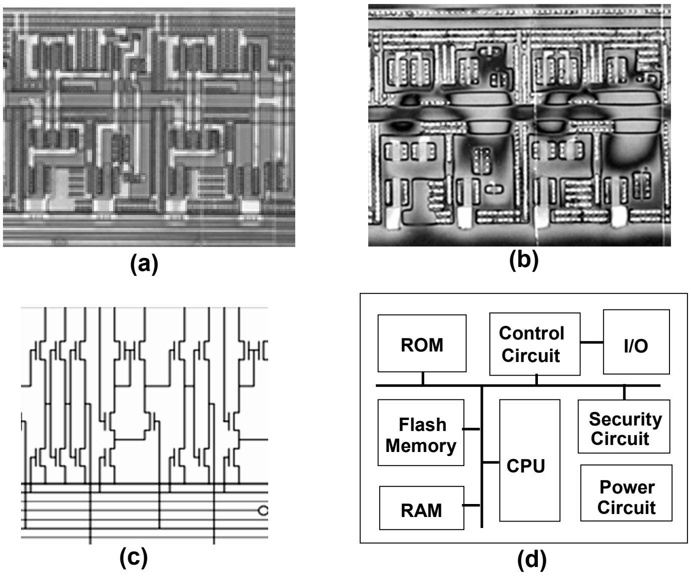


Fig. 16 Example circuit diagrams and architecture analysis. (a) & (b): chip surface after successive lapping. (c): circuit diagram and (d): block diagram.

V. 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 idea is summarized as Fig 17 and Fig. 18.

The attacker's integral skill ranks are defined as Fig. 17. To express the attacker's knowledge on a particular field and degree of experience we use symbols α, β, and γ that respectively means " expert" > "proficient" > "sufficient" levels. Then the attacker's skill ranks "the expert class", "the first class", "the second class", "the third class", "the fourth class" and "the fifth class" are defined. For example, the "the expert class" skill rank means that the attacker has "expert = α" level skills for LSI architecture, logic and analog circuit operation, memory circuit operation, memory cell structure, process technology, failure analysis technology, and measurement technology, and has at least 15-year experience. On the other hand, "the fourth class" skill rank means that the attacker has "sufficient = γ" level skills for logic and analog circuit operation and measurement technology and has "proficient = β" level skills for memory circuit operation, memory cell structure, and failure analysis technology, as well as at least 5-year experience.

In Fig. 18, we show the tentative candidate of five security levels of LSI chips as A, B, C, D, and E. Current average failure analysis capability may correspond to level C. Thus we marked a parenthesized number next to each symbol expressing the level. Level "Beyond" means the security level that is not attacked by today's failure analysis technologies.

Our attempt of classifying the security levels of LSI chips is not yet matured and should be improved based on much discussion.

VI. 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 bu means of high-bandwidth luminescence detection," Microelectronics Reliability, Vol. 43, pp. 1669-1674, 2003.

Skill Rank Skill component	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   α > β > γ

Fig. 17 Definition of Skill Ranks.

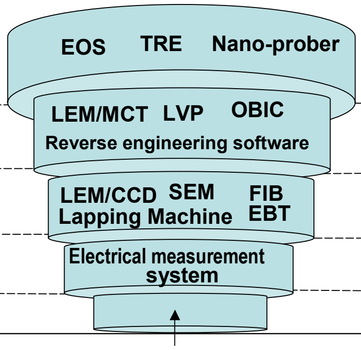
Security level	Necessary FA equipment	Equipment total cost [M$]	Skill rank
Beyond	Unknown (today)	?	?
A (+2)	 EOS TRE Nano-prober	10+6	Expert
B (+1)	LEM/MCT LVP OBIC Reverse engineering software	6.5+3.5	1st
C (0)	LEM/CCD SEM FIB Lapping Machine EBT	2.5+4	2nd
D (-1)	Electrical measurement system	0.5+2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

Fig. 18 Classification of security level of LSI chips by FA equipment and skills of analyst. “Beyond” means the level non-attackable by today’s FA technologies.