Physical Attacks and Tamper Resistance

Agenda

- Last Time
  - Bison Spirit!!!
  - JTAG
- Quick Review of JTAG lecture.
- Review Schedule
- Project 3 & 4 SPA & DPA??
  - Goal is to assign it Monday.
- Begin new unit.

Classification of Physical Attacks

Physical Attacks

Invasive Attacks	Non-Invasive Attacks	Semi-Invasive Attacks
• Microprobing • Reverse Engineering	• Side-channel Attacks • Brute Force Attacks • Fault Injection Attacks • Data Remanence	• UV Attacks • Optical Fault Injection • Advanced Imaging Techniques • Optical Side-Channel Attacks

Non-Invasive Attacks

- Do not require *de-capsulation* or *de-layering* of the device, so it is non-destructive
  - Will not leave tamper evidence, so the use cannot be aware of the attack
- Do not require any initial preparation of the device under test
  - They can be done by tapping on a wire or plugging the device in the test chip.
- Easily reproducible, so they are not expensive
- It can take a lot of time to find an attack on any particular device.

Non-Invasive Attacks

Passive

- Side-Channel Attacks
  - Power Analysis Attacks
  - Timing Attacks
  - Electromagnetic Emission Attacks

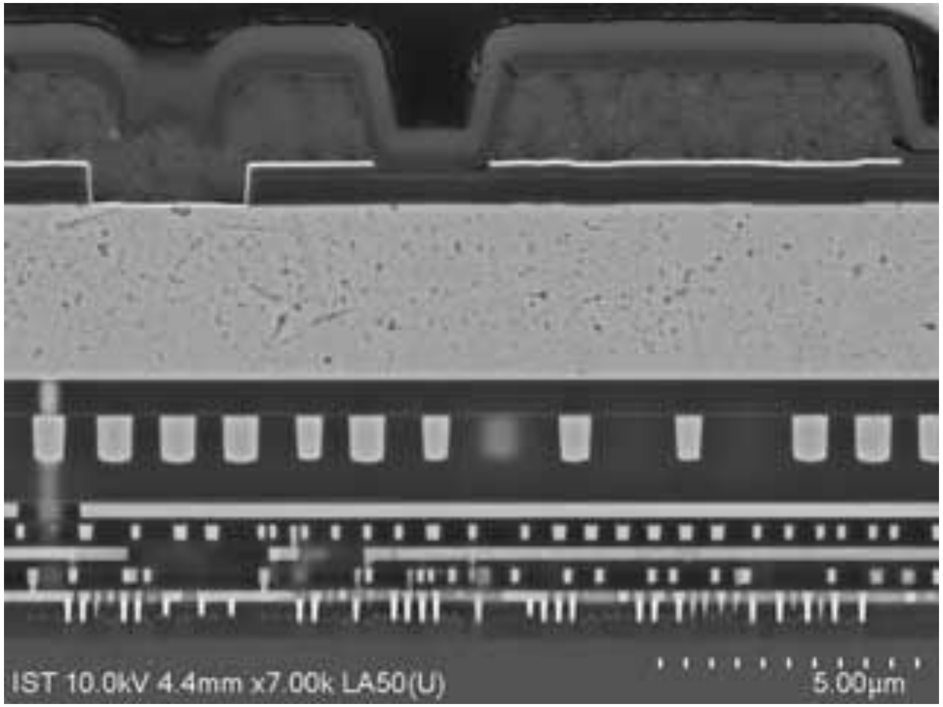
Active

- Brute Force Attacks
- Glitch Attacks
- Under-voltage and over-voltage attacks
- Current Analysis

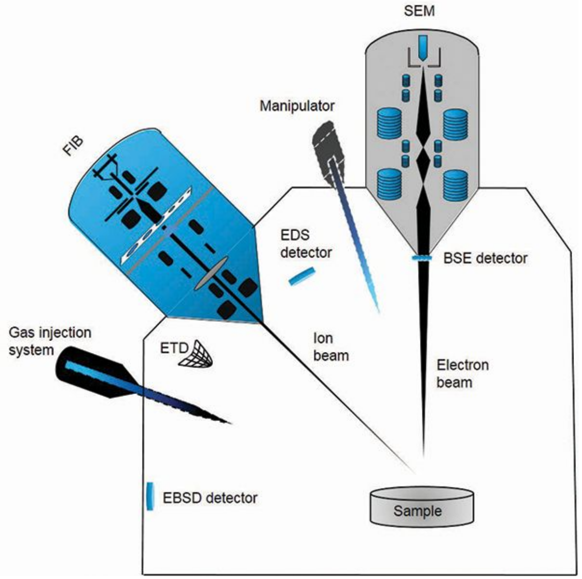
Invasive Attacks

- Expensive to perform
  - require expensive equipment, knowledgeable attackers and sometime significant amount of time
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - leave tamper evidence of the attack or even destroy the device
  - getting more demanding as the device complexity increases and the size shrinks (technology scales)
    - + At the same time, the quality of the imaging devices is increasing

Invasive Attacks



$20k - $3000k



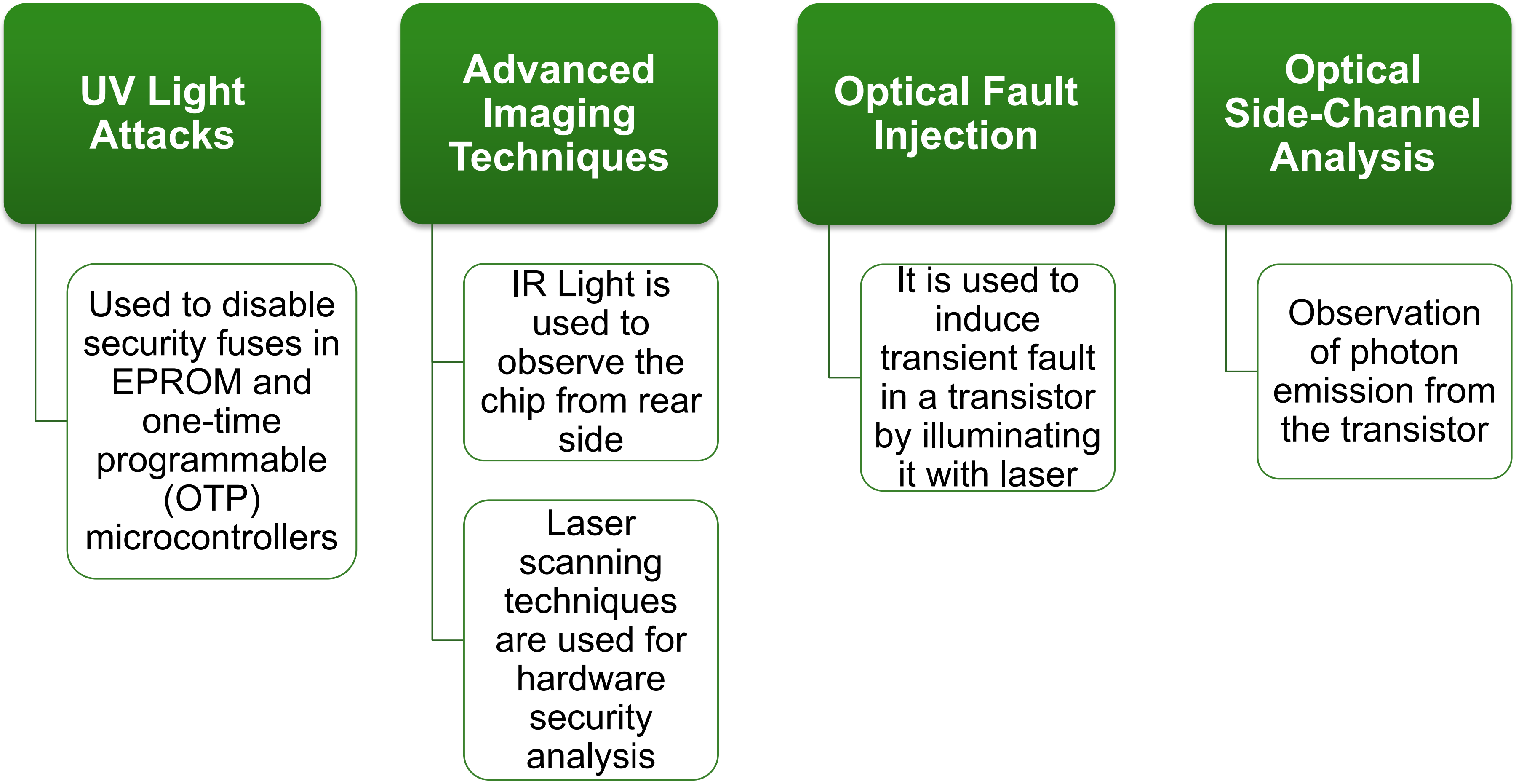
Invasive Attacks

- **Tools**
  - IC soldering/desoldering station
  - simple chemical lab and high-resolution optical microscope
  - wire bonding machine, laser cutting system, microprobing station
  - oscilloscope, logic analyzer, signal generator
  - scanning electron microscope and focused ion beam workstation

Semi-Invasive Attacks

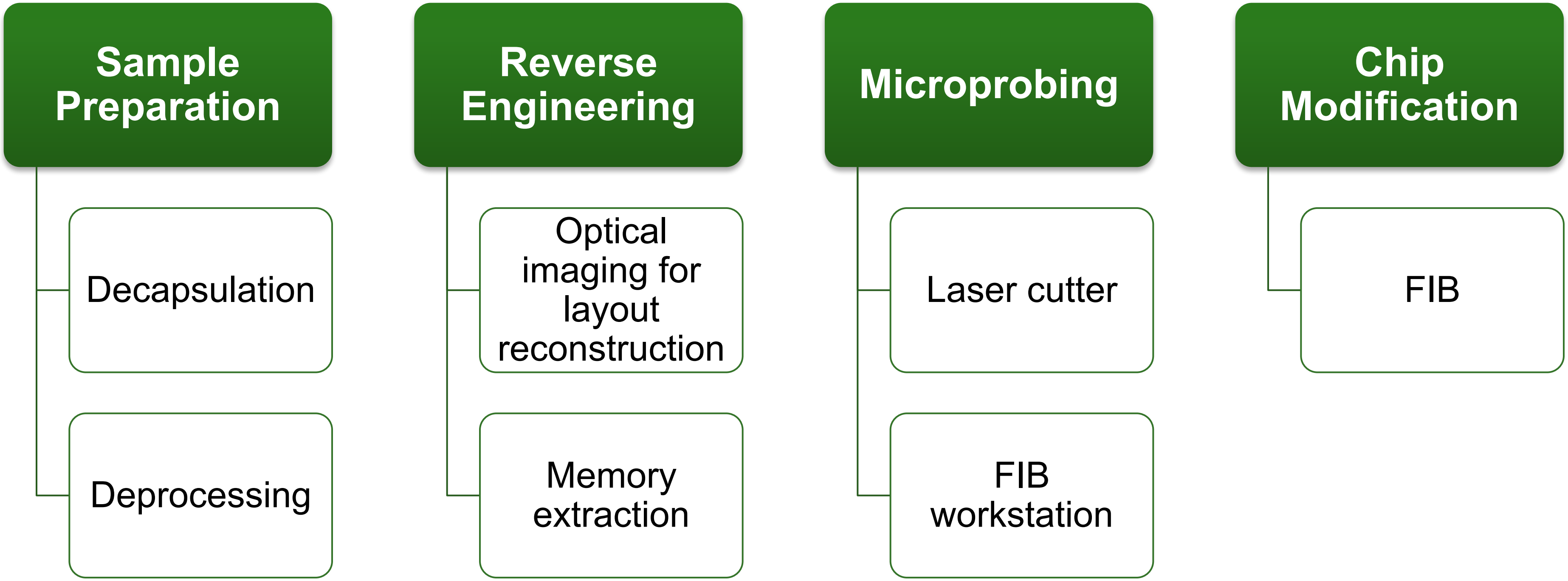
- Relatively new type of attack, it fills the gap between *non-invasive* and *invasive* attacks
- Similar to the invasive attacks, they require de-packaging of the device
- The attacker do not need to have expensive tools such as FIB.
- Such attacks are not entirely new
  - E.g., UV light is used to disable security fuses in EPROM for many years

Semi-Invasive



- **UV Light Attacks**
  - Used to disable security fuses in EPROM and one-time programmable (OTP) microcontrollers
- **Advanced Imaging Techniques**
  - IR Light is used to observe the chip from rear side
  - Laser scanning techniques are used for hardware security analysis
- **Optical Fault Injection**
  - It is used to induce transient fault in a transistor by illuminating it with laser
- **Optical Side-Channel Analysis**
  - Observation of photon emission from the transistor

Invasive Attacks



Sample Preparation

- Decapsulation
- Deprocessing

Reverse Engineering

- Optical imaging for layout reconstruction
- Memory extraction

Microprobing

- Laser cutter
- FIB workstation

Chip Modification

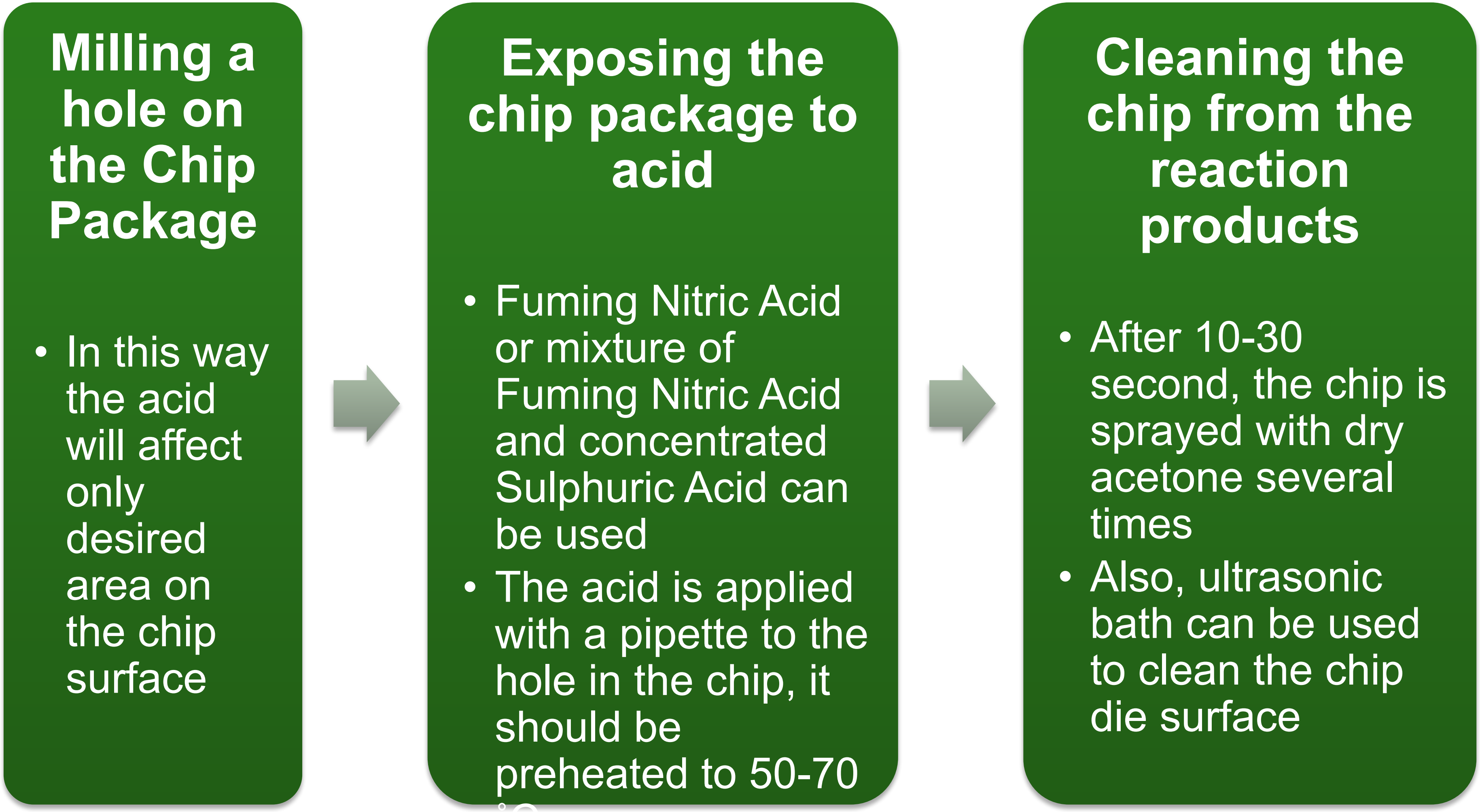
- FIB

Sample Preparation

- It starts with partial or full **decapsulation** of the chip to expose the chip die

- **Decapsulation** is the process of the removal of the chip package
  - It can be done easily by anyone who has low level chemistry knowledge
  - Only need to do some practice on a dozen chips

Manual Decapsulation



Milling a hole on the Chip Package

- In this way the acid will affect only desired area on the chip surface

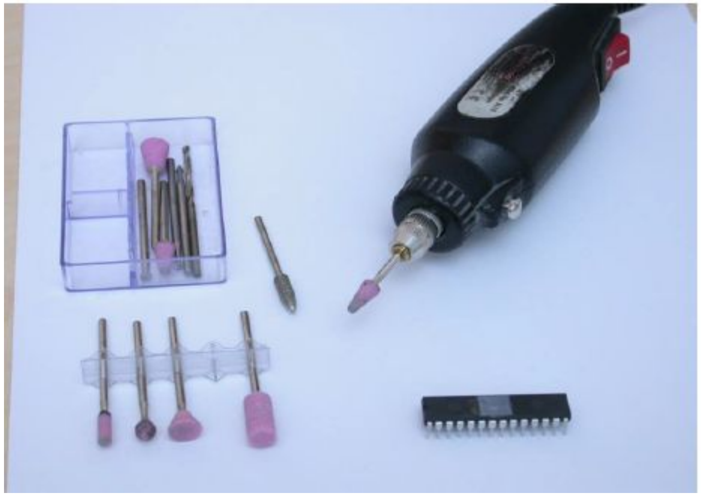
Exposing the chip package to acid

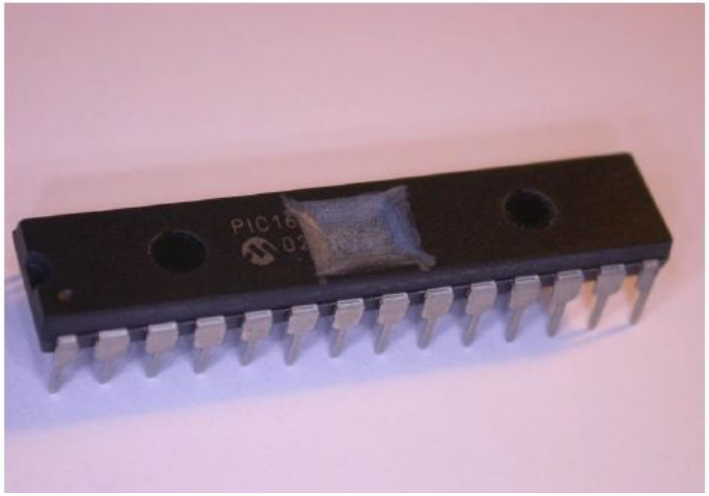
- Fuming Nitric Acid or mixture of Fuming Nitric Acid and concentrated Sulphuric Acid can be used
- The acid is applied with a pipette to the hole in the chip, it should be preheated to 50-70 °C

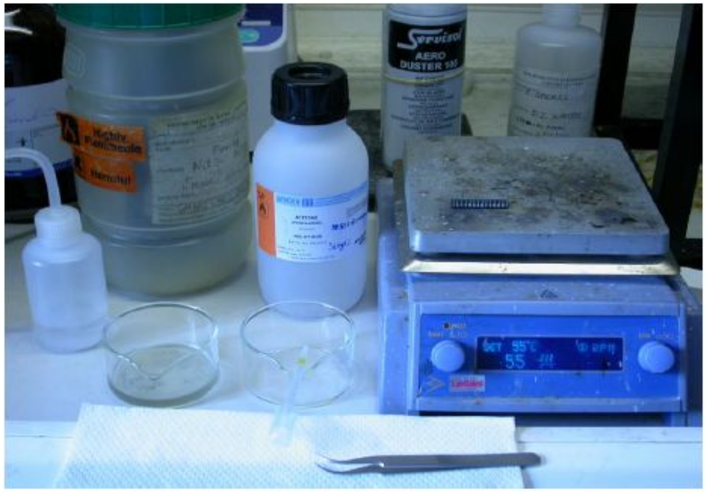
Cleaning the chip from the reaction products

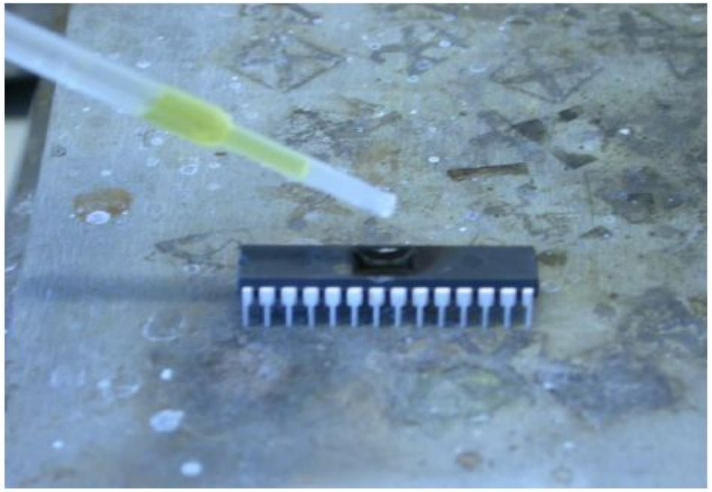
- After 10-30 second, the chip is sprayed with dry acetone several times
- Also, ultrasonic bath can be used to clean the chip die surface

Manual Decapsulation

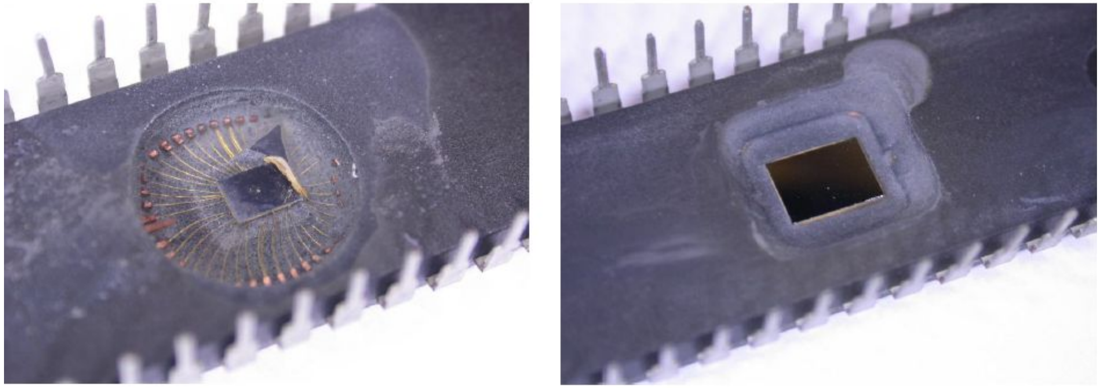








Manual Decapsulation



- **Decapsulation can be done from the rear side of the chip**
  - Access to the chip die can be established without using any chemical
  - It requires to mill down to the copper plate which can be then removed mechanically

Automated Decapsulation

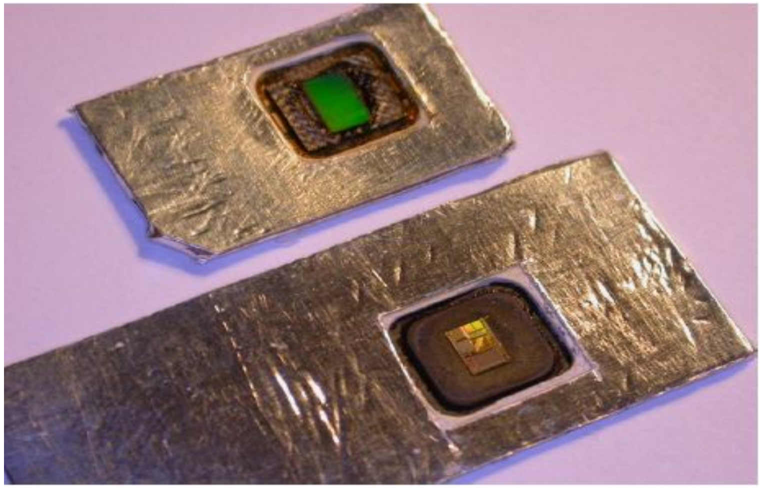
For large quantities, automated decapsulation systems can be used.

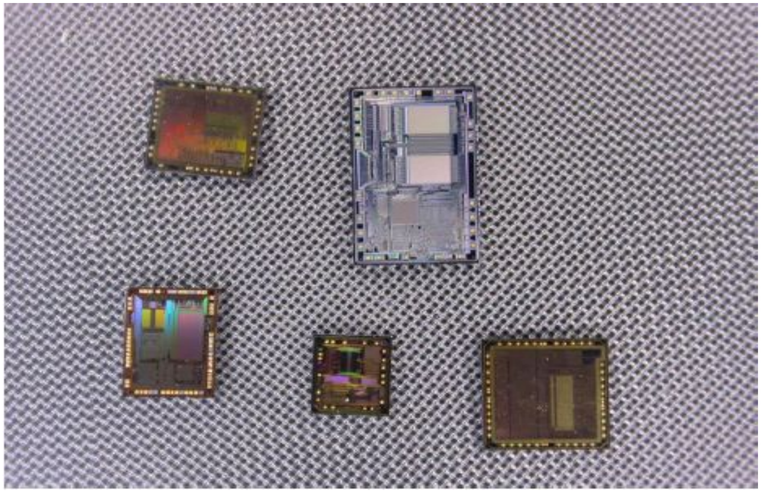
- Very little skill and experience is required to operate it
- Cost around $15,000
- Also, they consume ten times more acid than the manual decapsulation, so the disposal of the waste should be done in proper way

Nippon Scientific, PA103

Example Decapsulation

- The same partial decapsulation can be applied to smart card
- Not all of them may maintain their electrical integrity
- Generally, smart cards are decapsulated completely





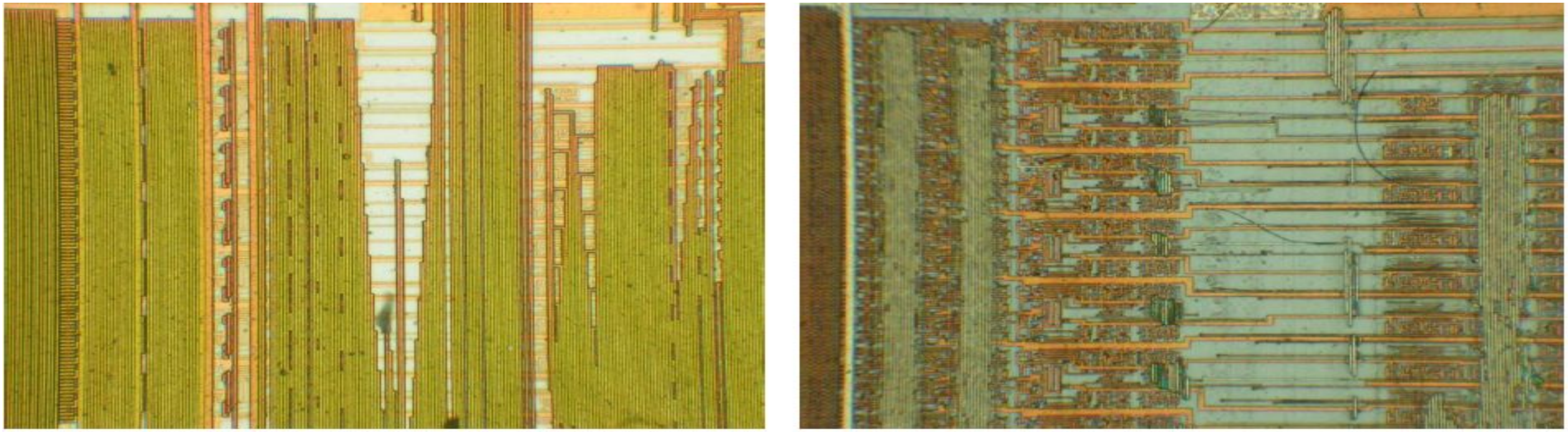
Sample Preparation

- **Deprocessing** is the opposite process of the chip fabrication
- It has two main applications:
  - Removing passivation layer to expose metal layers for microprobing attack
  - Gaining access to the deep layers to observe internal structure of the chip
- Three basic deprocessing methods are used:
  - Wet chemical etching
  - Plasma etching, also known as dry etching
  - Mechanical polishing

Deprocessing

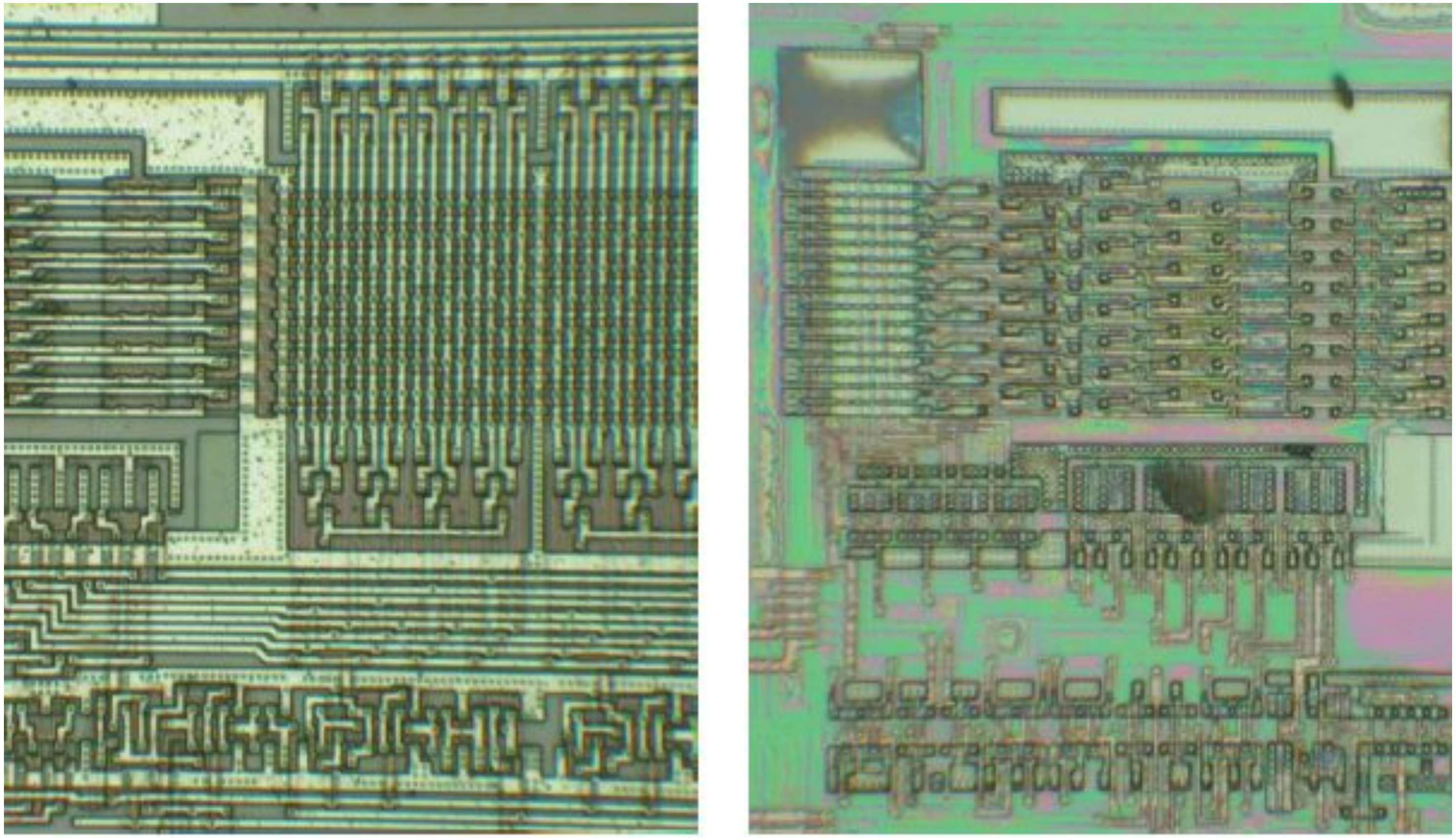
- **Wet Chemical Etching**
  - Each layer is removed by specific chemicals
  - Its downside is its uniformity in all directions
  - Each type of material needs certain etchants to be used
  - Nitrox wet etchant is one of the most effective etching agents for silicon nitride and silicon dioxide passivation layers which selectively removes the passivation layers of integrated circuits while preserving full device functionality.

Deprocessing



Microchip PIC16F76 microcontroller. The top metal layer is removed exposing the second metal layer.

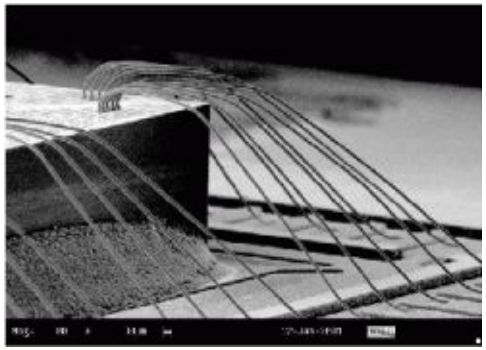
Deprocessing



Motorola MC68HC705C9A microcontroller. The metal layer is removed exposing the polysilicon and the doping layers.

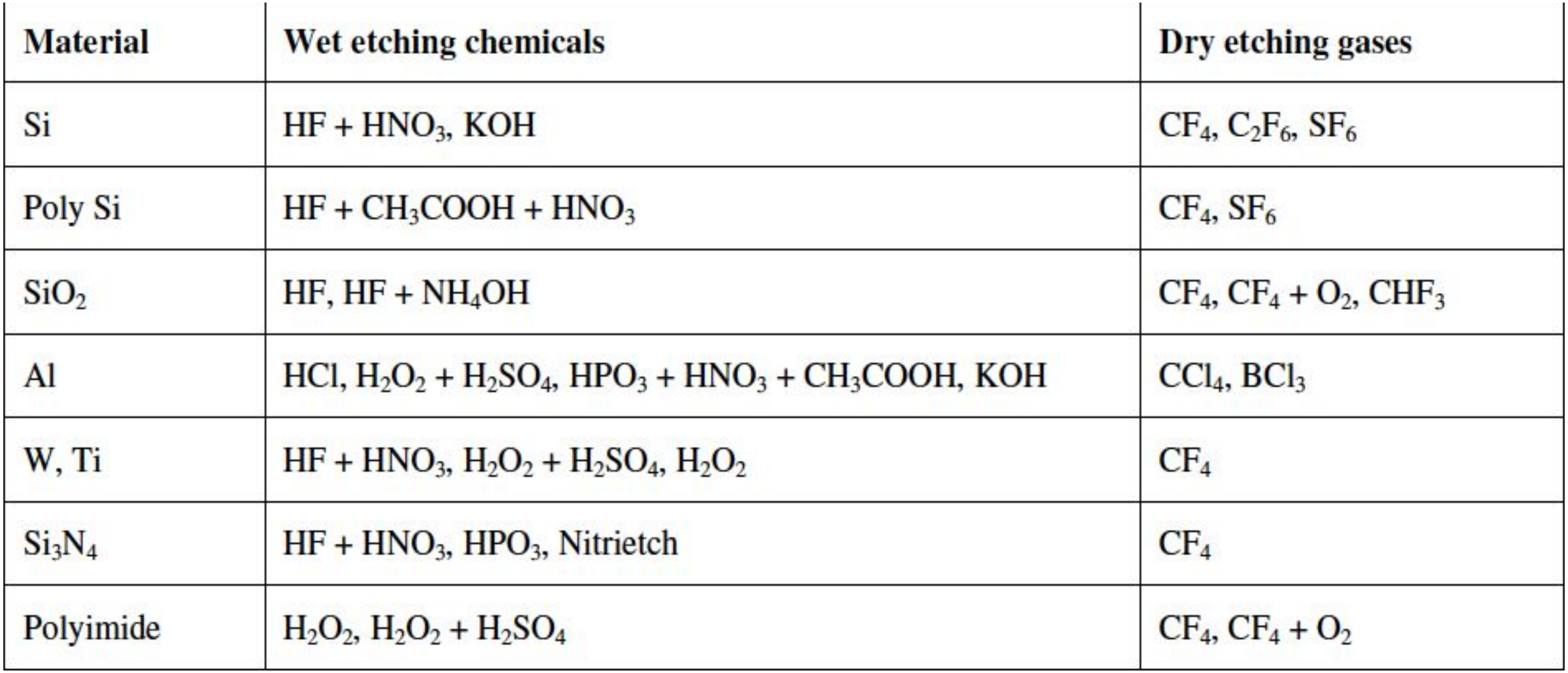
Deprocessing

- **Plasma Etching**
  - Uses radicals created from gas inside a special chamber.
  - Only the surfaces hit by the ions are removed
  - Similarly, each type of material needs certain enchant



- **Mechanical Polishing**
  - Performed with the use of abrasive materials
  - Time-consuming and requires special machines

Etching Agents for Wet Chemical and Plasma Etching



Material	Wet etching chemicals	Dry etching gases
Si	$HF + HNO_3$, KOH	CF_4, C_2F_6, SF_6
Poly Si	$HF + CH_3COOH + HNO_3$	CF_4, SF_6
SiO_2	HF, $HF + NH_4OH$	CF_4, $CF_4 + O_2$, CHF_3
Al	HCl, $H_2O_2 + H_2SO_4$, $HPO_3 + HNO_3 + CH_3COOH$, KOH	CCl_4, BCl_3
W, Ti	$HF + HNO_3$, $H_2O_2 + H_2SO_4$, H_2O_2	CF_4
Si_3N_4	$HF + HNO_3$, HPO_3, Nitrietch	CF_4
Polyimide	H_2O_2, $H_2O_2 + H_2SO_4$	CF_4, $CF_4 + O_2$

Reverse Engineering

- RE is used for understanding the **structure** of the device and its **functioning**
- For ASIC, it means locations of all the **transistors** and **interconnections**
- **All the layers** of the chip are removed one by one in reverse order and photographed to determine the internal structure of the chip
- Eventually, by processing obtained information, circuit netlist can be created and used to simulate the device

Reverse Engineering

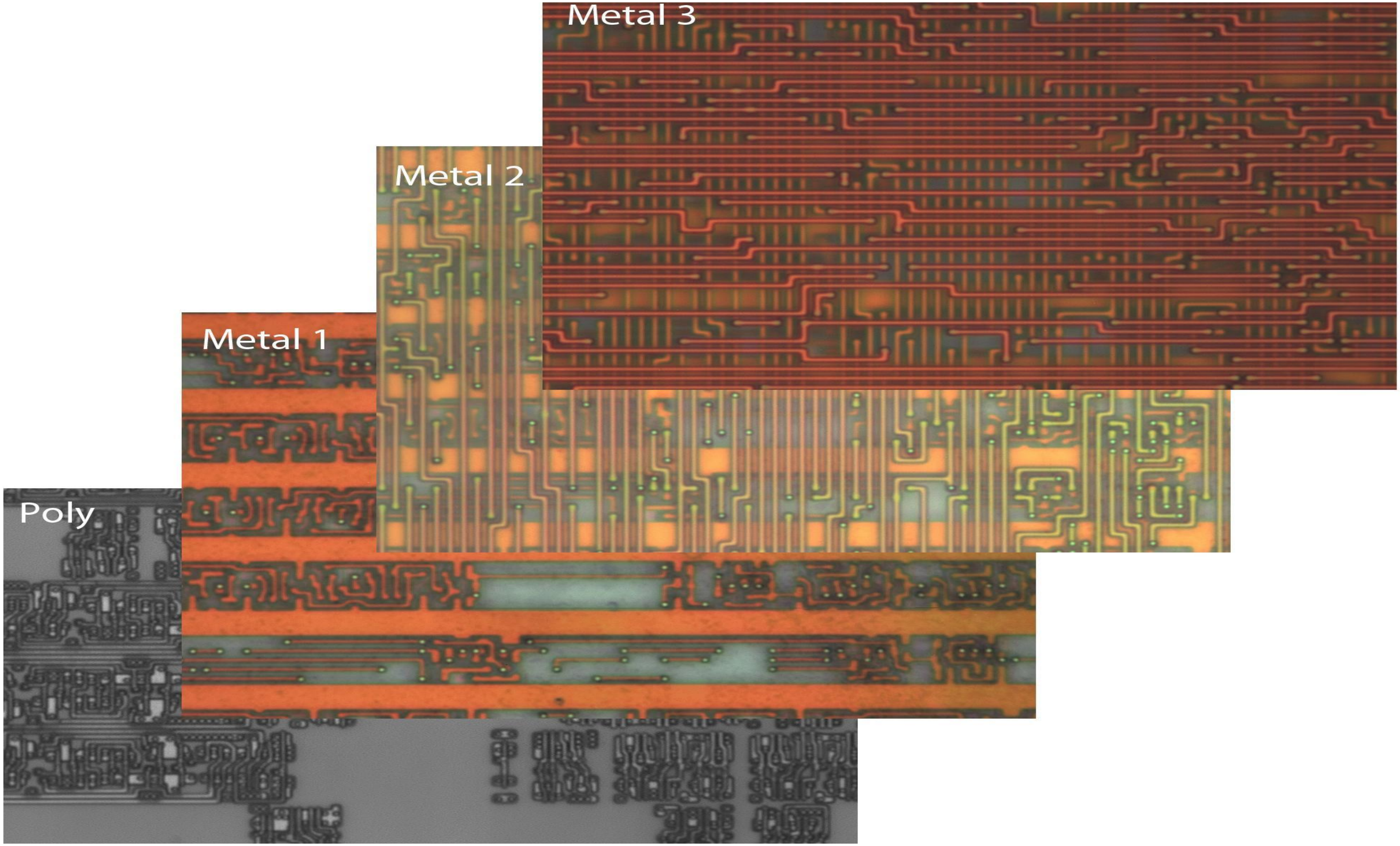
- It is tedious and time-consuming process
- For the smartcards and microcontrollers, both **structural** and **program-code** reverse engineering is required.
  - First, security protection should be understood by **partial reverse engineering**
  - If memory bus encryption was used, the hardware responsible for this should be reverse engineered.
- For the CPLDs and FPGAs, even if the attacker obtained the configuration bitstream, he or she needs to spend a lot of time to simulate it

Reverse Engineering: Imaging

- **Optical Imaging:**
  - For reverse engineering the silicon chips down to 0.18 µm feature size, an optical microscope with a digital camera can be used

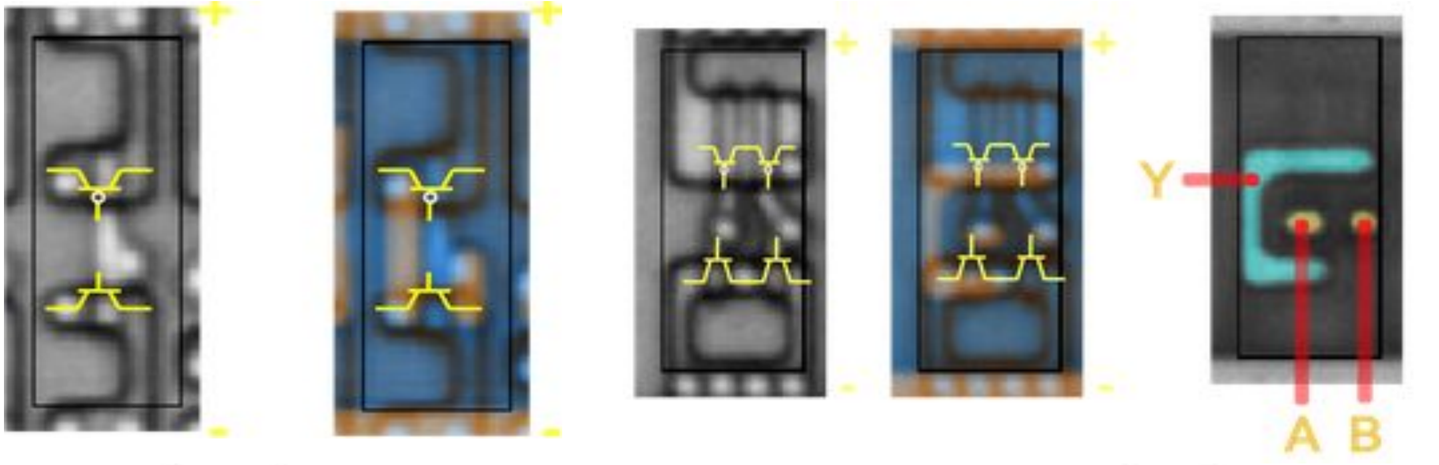
- **Scanning Electron Microscopy (SEM):**
  - For semiconductor chips fabricated with 0.13 µm or smaller technology, images are created using a SEM which has a resolution better than 10 nm.

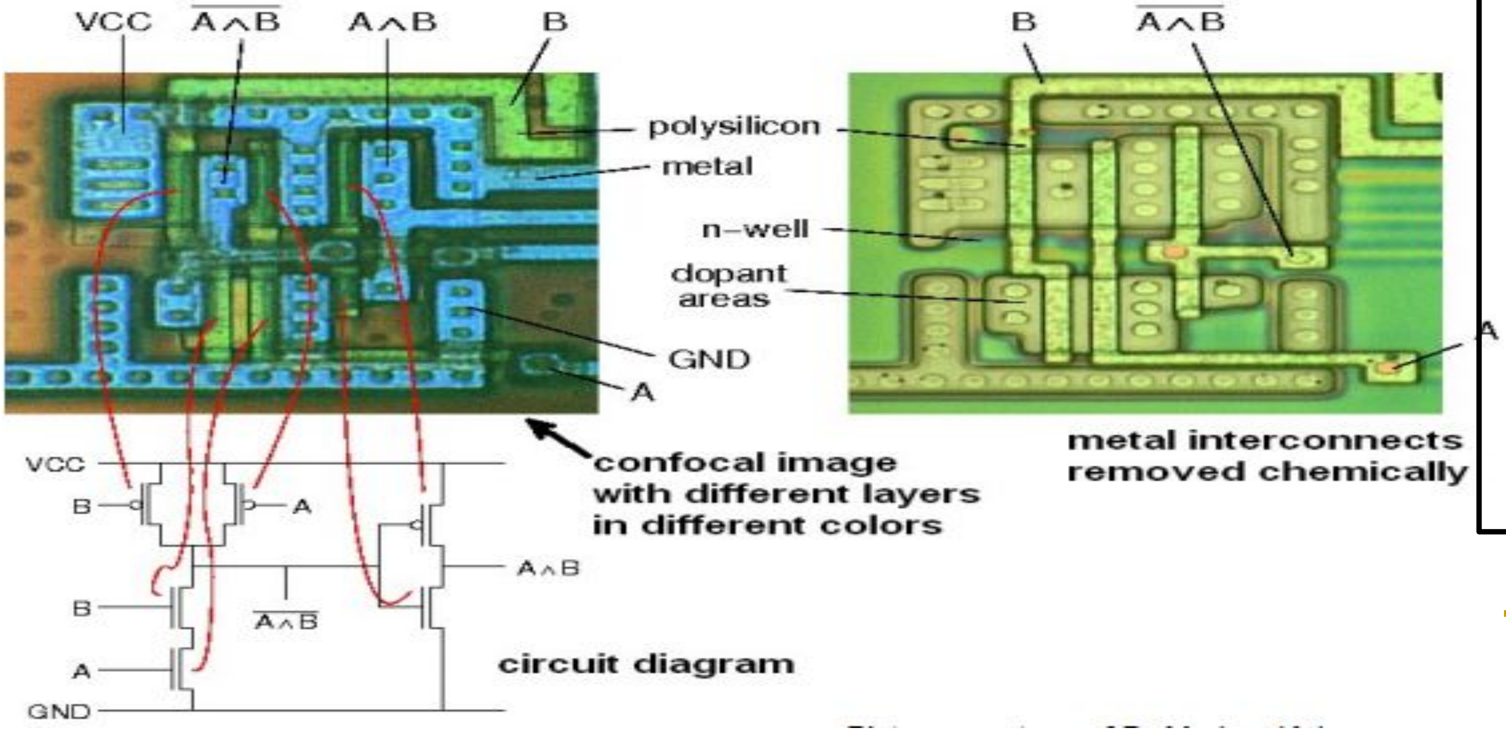
Layer by Layer Imaging



Flylogic.net/blog

Reverse Engineering

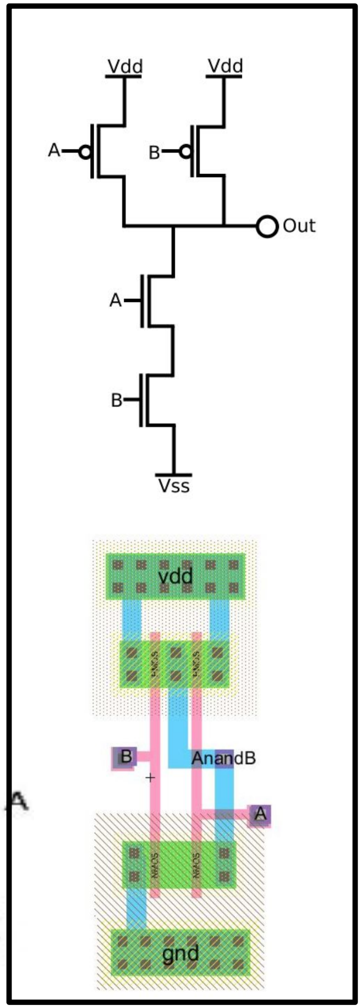




confocal image with different layers in different colors

metal interconnects removed chemically

circuit diagram



NAND Gate

Reverse Engineering: Memory Extraction

- **Memory Extraction from Mask ROMs**
  - Only possible for certain type of Mask ROM memory
  - NOR Mask ROM with active layer programming used in Motorola MC68HC705P6A Microcontroller can be read by removing the top metal layer
  - But, same Microcontroller with newer technology requires detailed deprocessing

Reverse Engineering: Memory Extraction

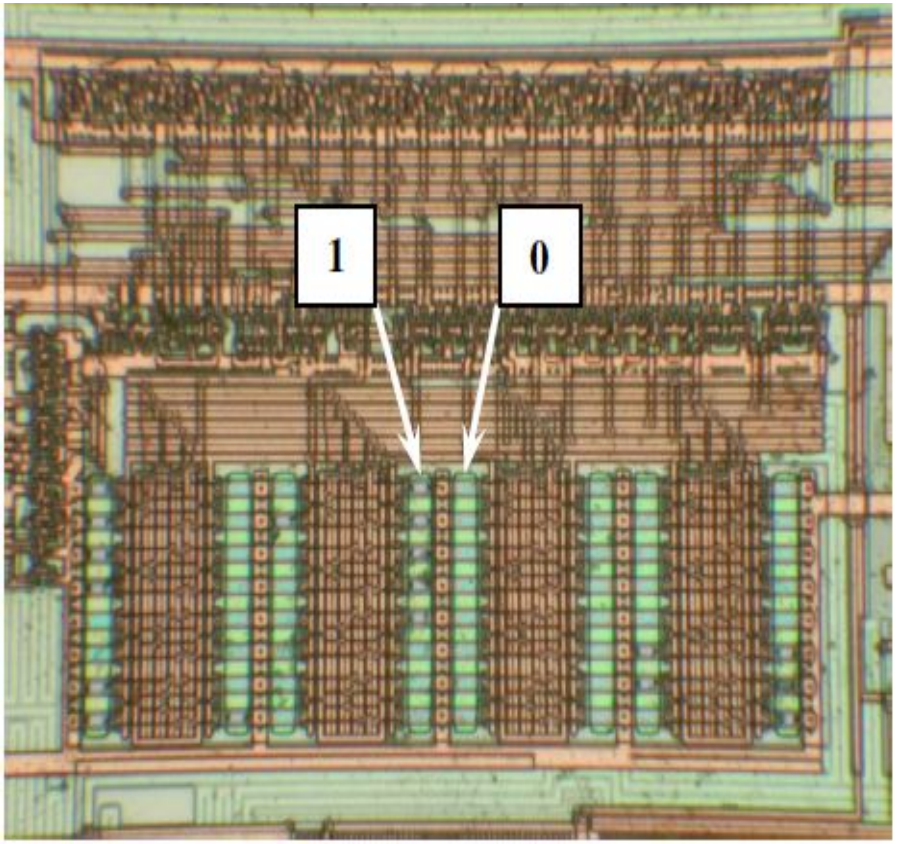


Figure 17. Laser ROM in Dallas DS1961S iButton chip [49]. Information can be read optically and altered with a laser cutter

The logic state is encoded by the absence or presence of the nor transistor OR the absence or presence of the a via plug from bit-line to the active area of a transistor.

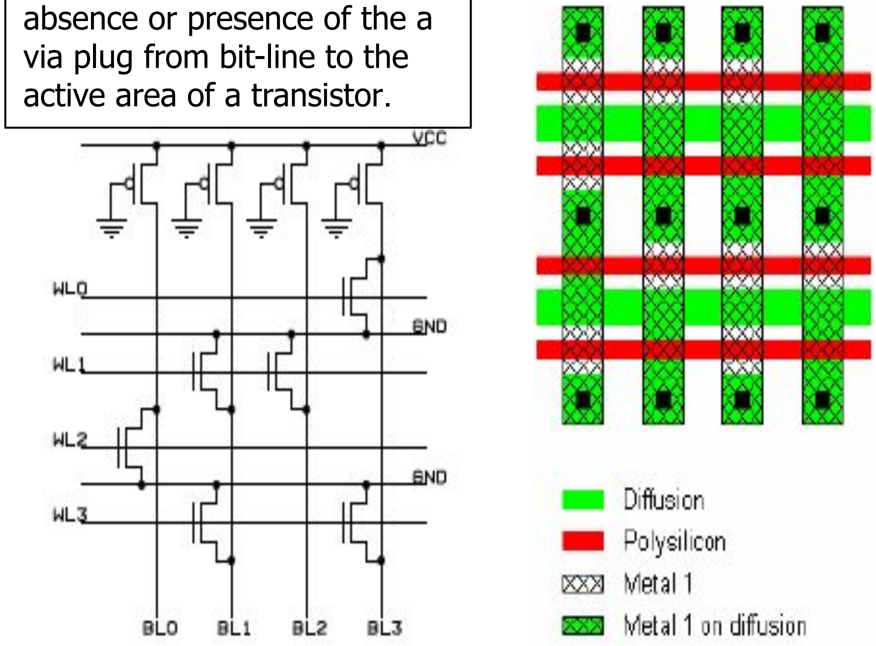


Figure 18. Configuration and layout of MOS NOR ROM with active layer programming. This type of memory can be read optically

Reverse Engineering

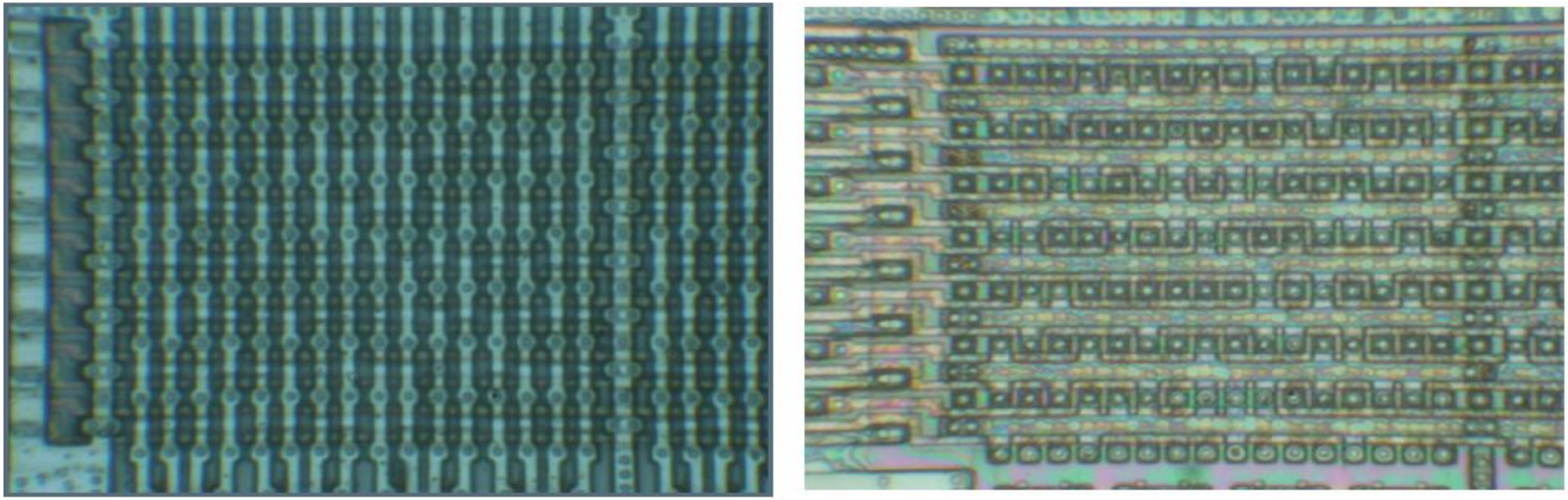


Figure 60. Optical image of the Mask ROM inside MC68HC705C9A microcontroller before and after wet chemical etching. 500× magnification

Reverse Engineering

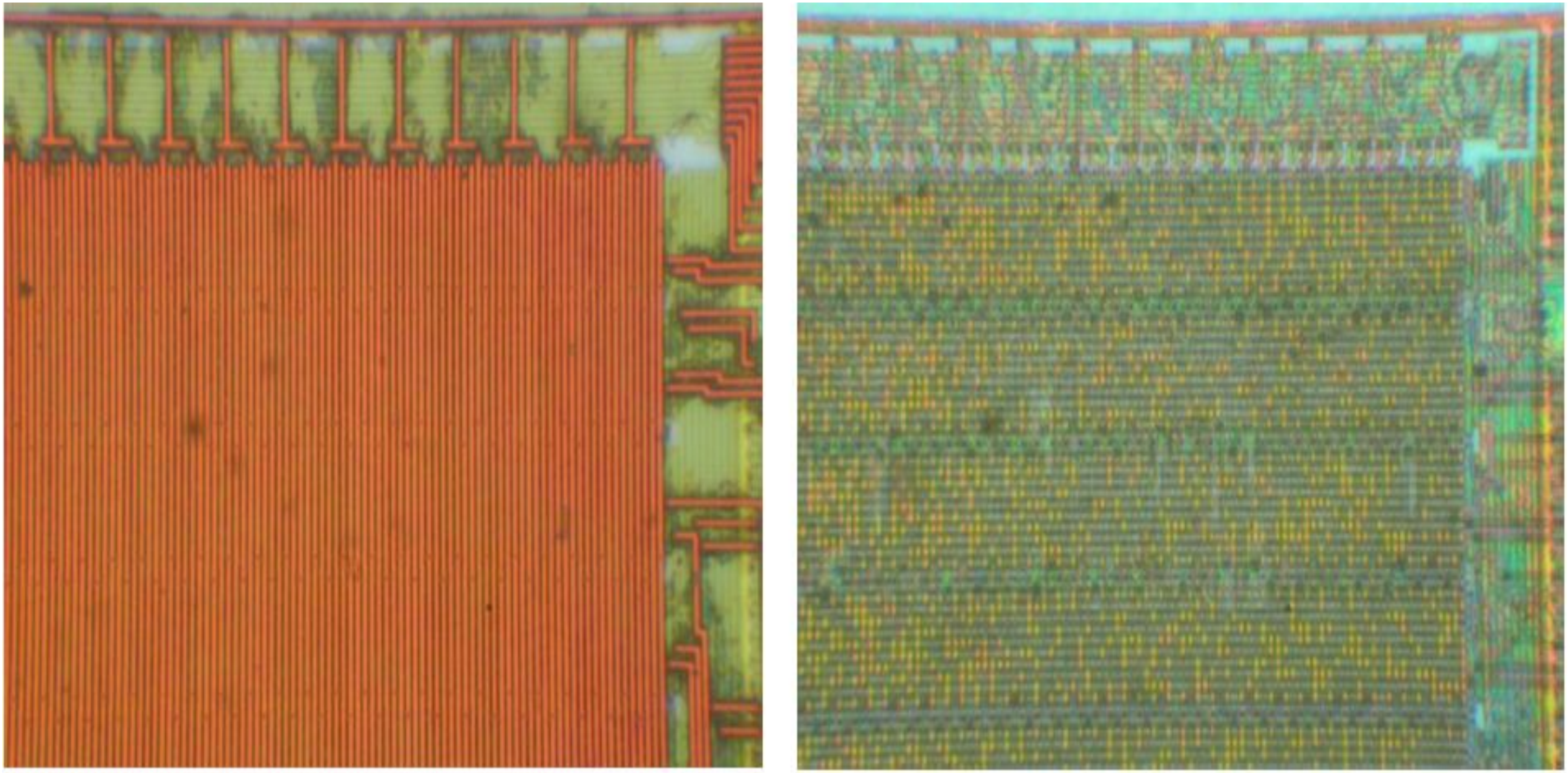


Figure 61. Optical image of the Mask ROM inside µPD78F9116 microcontroller before and after wet chemical etching. 500× magnification

Reverse Engineering

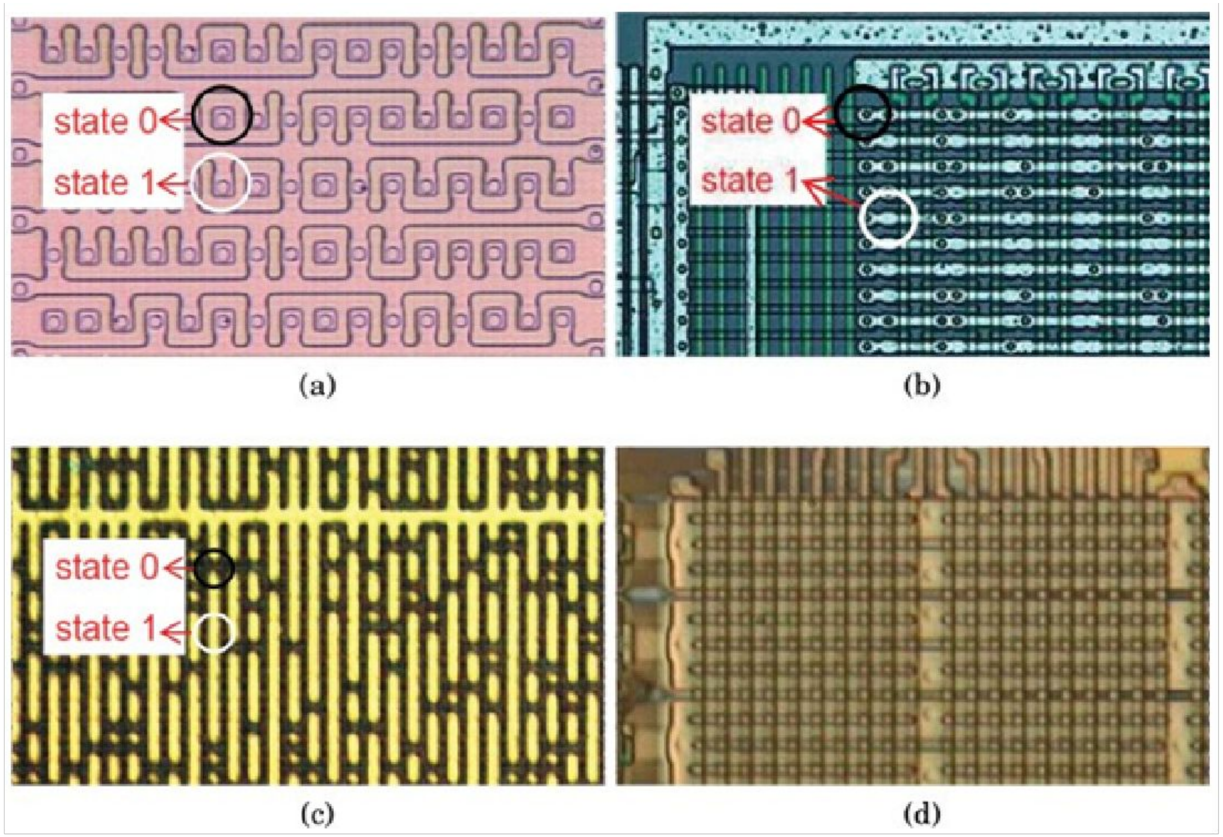


Figure 16: Optical inspection of active-layer programming ROM [63](a), contact- layer programming ROM [28] (b), metal-layer programming ROM [64](c), and implant programming ROM before selective etch [64](d).

Reverse Engineering

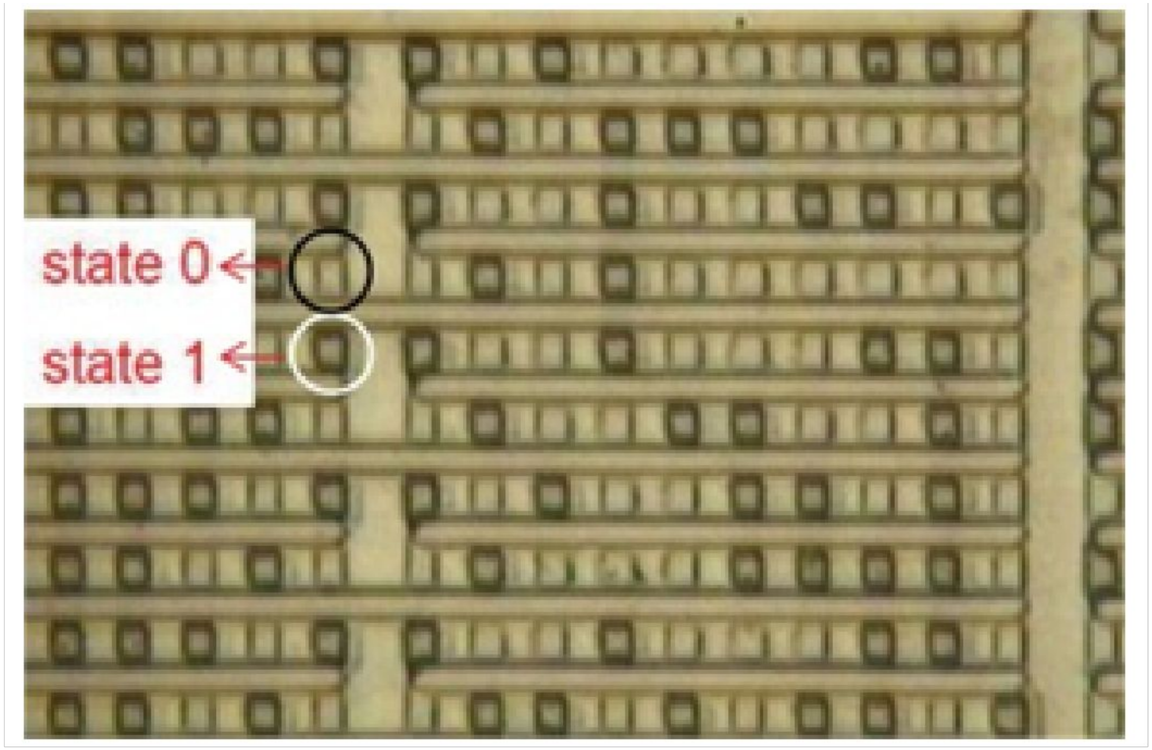


Figure 17: Optical inspection of implant programming ROM after selective etch [64].

Agenda

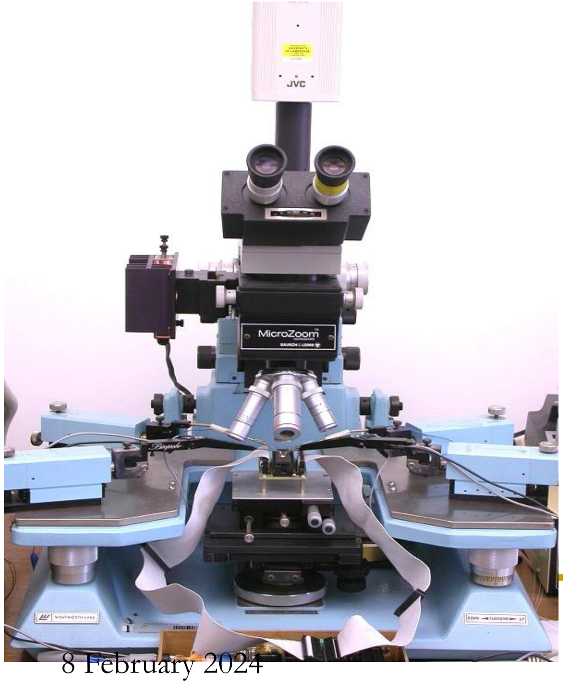
- Last Time
  - Review Last Class
- Review Schedule
- Project 3 will be JTAG.
- Next time Side Channel Analysis

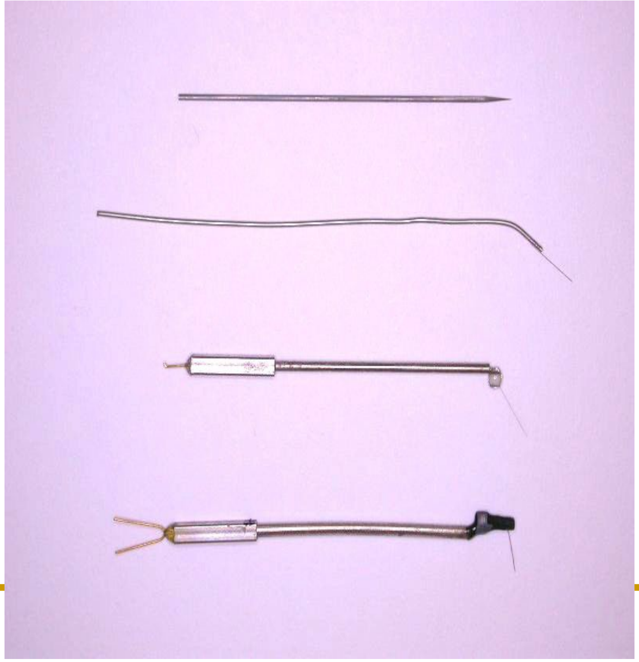
Invasive Attacks: Microprobing

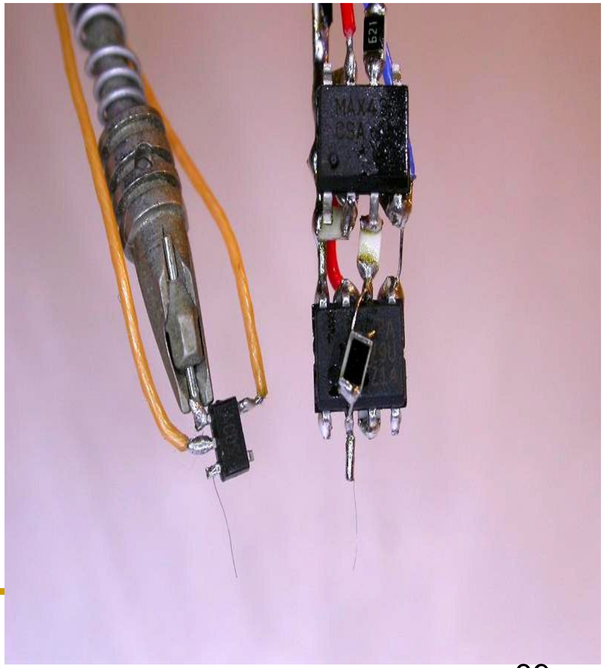
- **Microprobing**
  - Could be used for both *Confidentiality* and *Integrity* violations
    - eavesdropping on signals inside a chip (Confidentiality violation)
      - can be used for extraction of secret keys and memory contents
    - injection of test signals and observing the reaction (Integrity violation)
  - laser cutter can be used to remove passivation and cut metal wires

Invasive Attacks: Microprobing

- **Tools**
  - The most important tool is microprobing station. It consists of five elements
    - a microscope, stage, device test socket, micromanipulators and probe tips.







Invasive Attacks: Microprobing

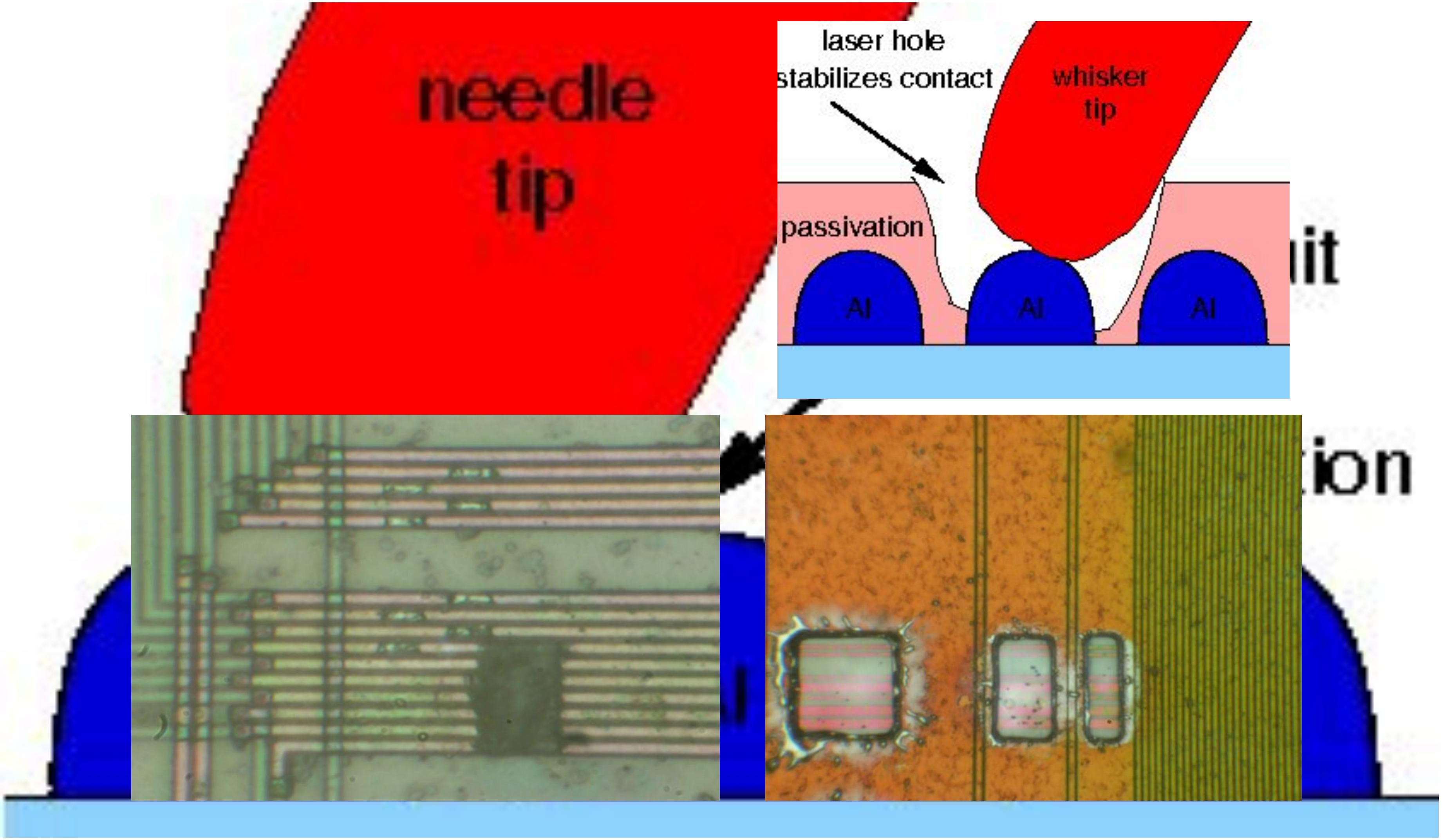
- **Microprobing is applied to the internal CPU data bus**
  - Difficult to observe whole data bus all at once
  - There are limited number of probes
  - Two to four probes are used to observe data signals which are combined as a whole data trace later.

Microprobing: Laser Cutting

- It is used to remove passivation layer to observe the metal layer
- Laser Cutting Systems consist of:
  - laser head mounted on camera port of a microscope
  - submicron-precision stage to move the sample
- Carefully dosed laser flashes remove patches of the passivation layer with micrometer precision

VISIBLE AND INVISIBLE LASER RADIATION
LASER CUTTER MUST NOT BE OPERATED WITHOUT MICROSCOPE
CLASS 3B LASER PRODUCT
AVOID EXPOSURE TO BEAM

Microprobing: Laser Cutting



Microprobing: FIB Workstation

- The devices fabricated with lower technology node needs more sophisticated tools to establish contacts with the interconnect wires
- FIB stations can be used to create test point, imaging and repairing
- Also, FIB can mill holes and cut the wires

FIB Workstation

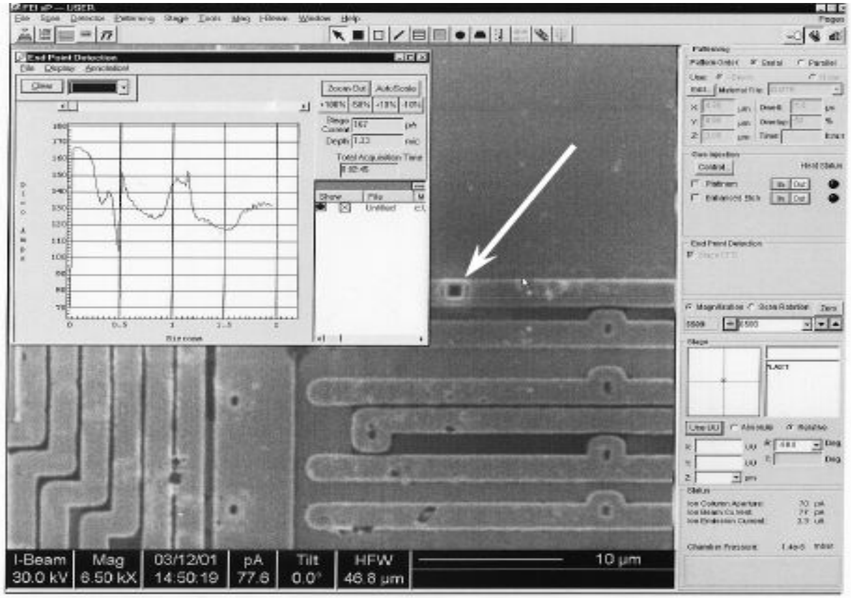

I-Beam 30.0 kV | Mag 6.50 kX | 03/12/01 14:50:19 | pA 77.6 | Tilt 0.0° | HFW 46.8 µm | 10 µm

Figure 68. The process of milling the hole using FIB

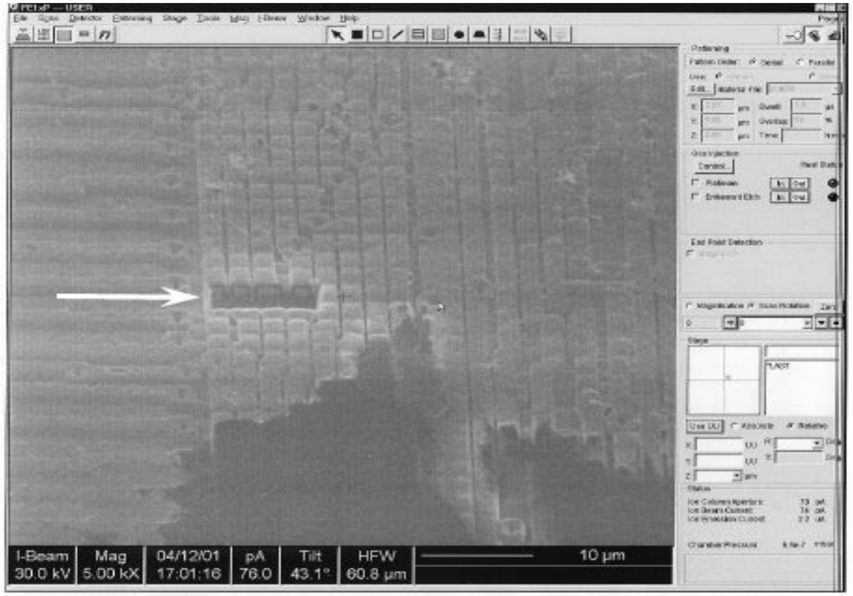
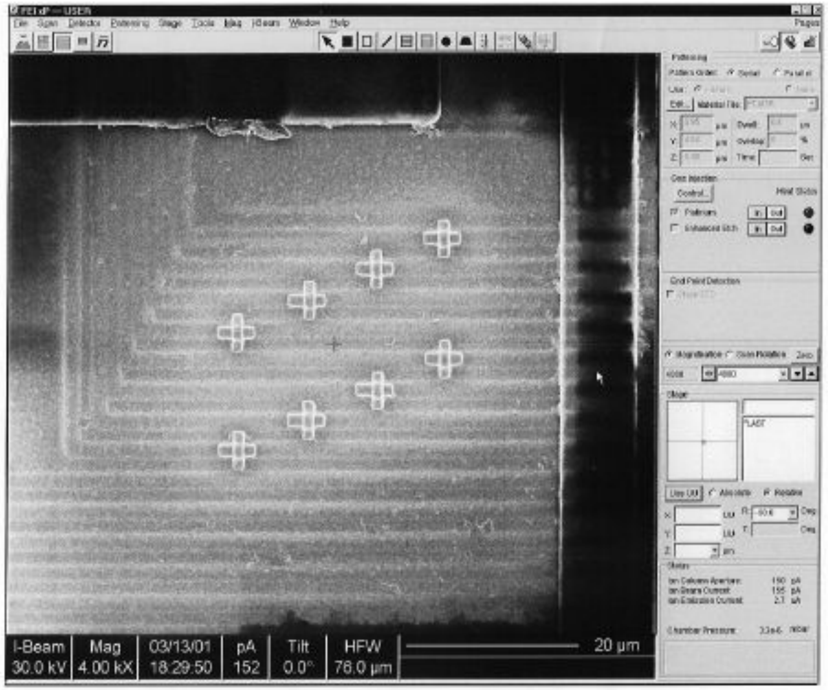

I-Beam 30.0 kV | Mag 5.00 kX | 04/12/01 17:01:16 | pA 76.0 | Tilt 43.1° | HFW 60.8 µm | 10 µm

Figure 69. Cutting the wires using FIB

A hole that is milled by FIB workstation. You can create really tiny holes on the chip die with FIB

wire cutting with FIB. It can be used for chip modification attacks to disable the security circuitry.

FIB Workstation



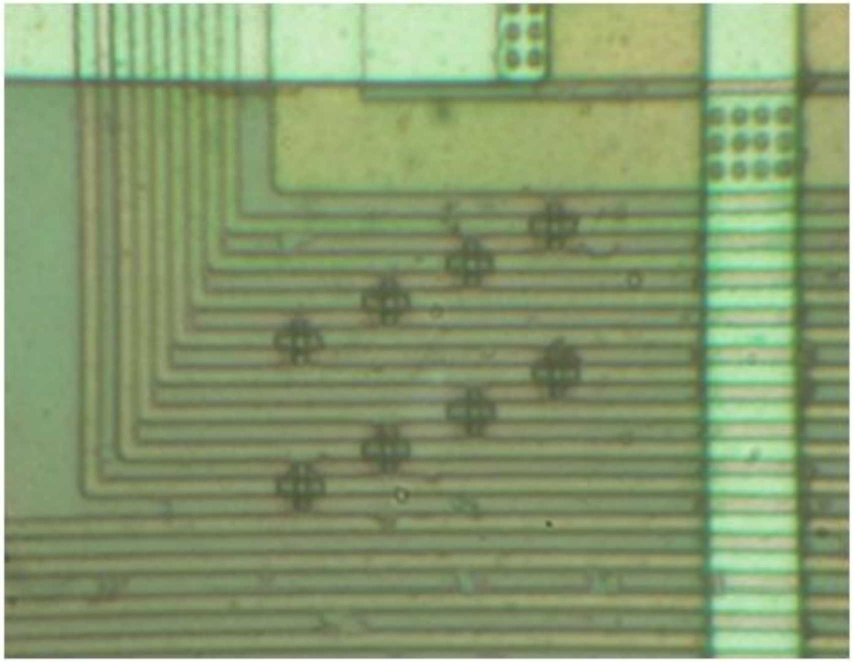


Figure 70. Test points created under FIB and optical image of these points

Test points created by FIB. Without removing any layer, by creating test point over the chip surface, probing attacks can be performed.

An image created by FIB

Invasive Attacks: Chip Modification

- It is used to disable security protection circuitry
  - By cutting one of the internal metal interconnection wires
  - By completely destroying the circuit associated with the security protection using a laser cutter
- For more sophisticated attacks FIB is used
  - Connecting the wire that transmits the security state to either the ground or the supply line.
- Chip modification always requires at least partial reverse engineering of the chip to find the point for possible attack.

Invasive Attacks: Chip Modification

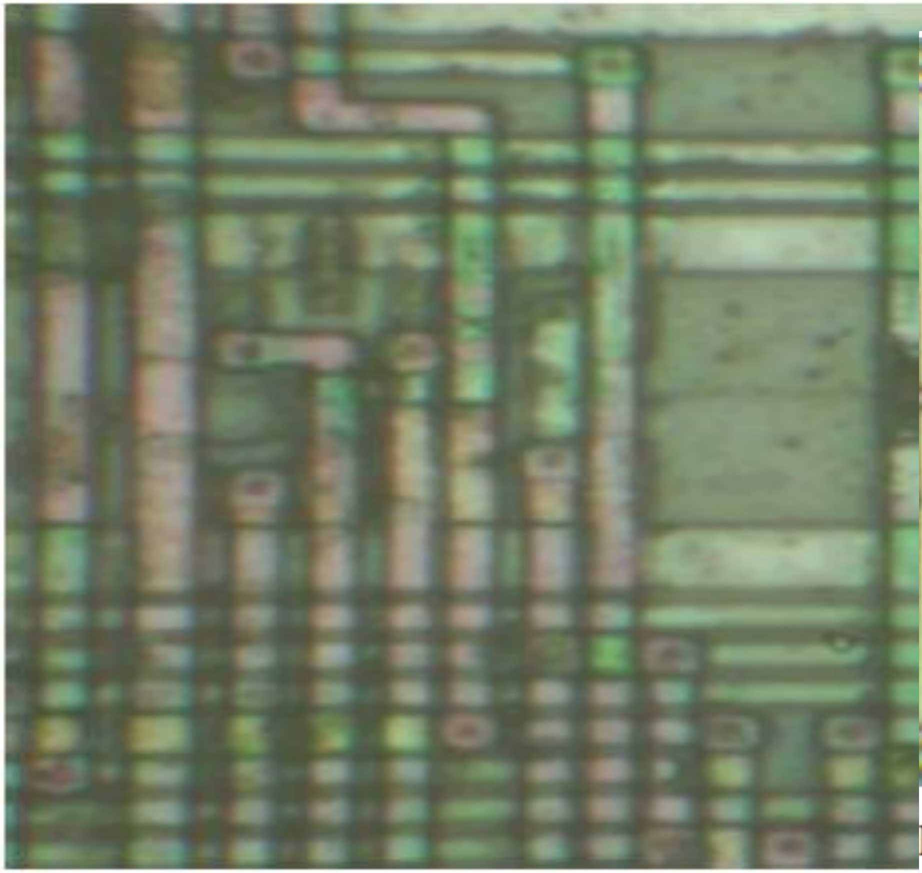


Figure 71. Cutting a single microcontroller disables the security. 1000× magnification

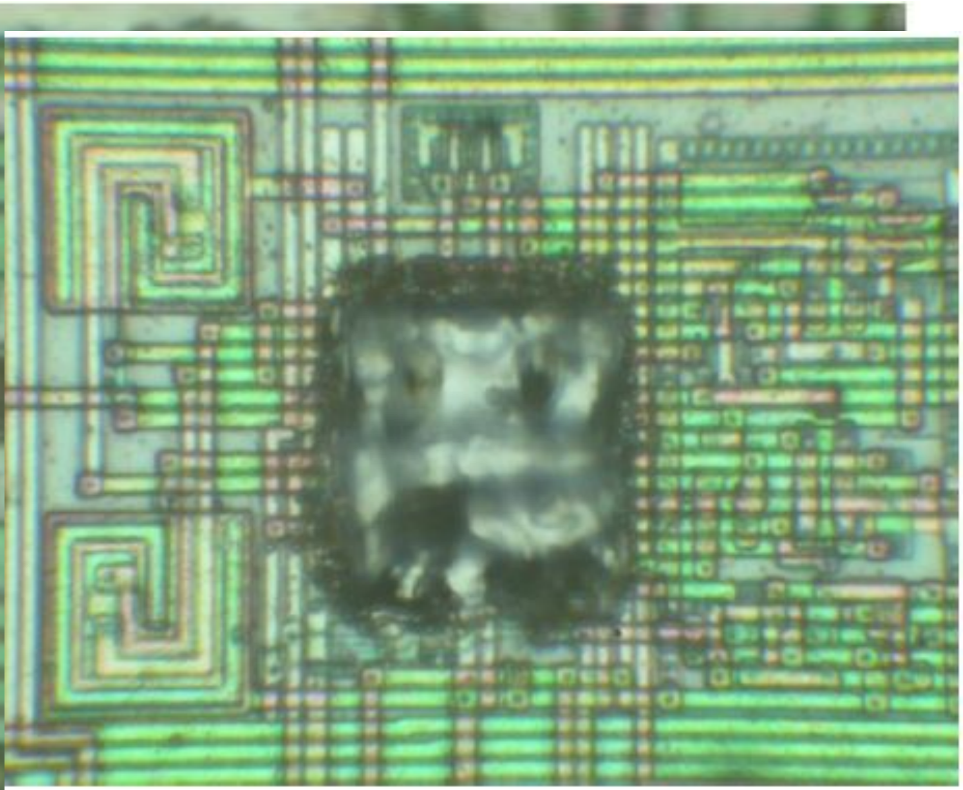


Figure 72. Disabling the security in the PIC16F628 microcontroller by destroying the fuse control circuit with a laser cutter. 500× magnification

Invasive Attacks: Chip Modification

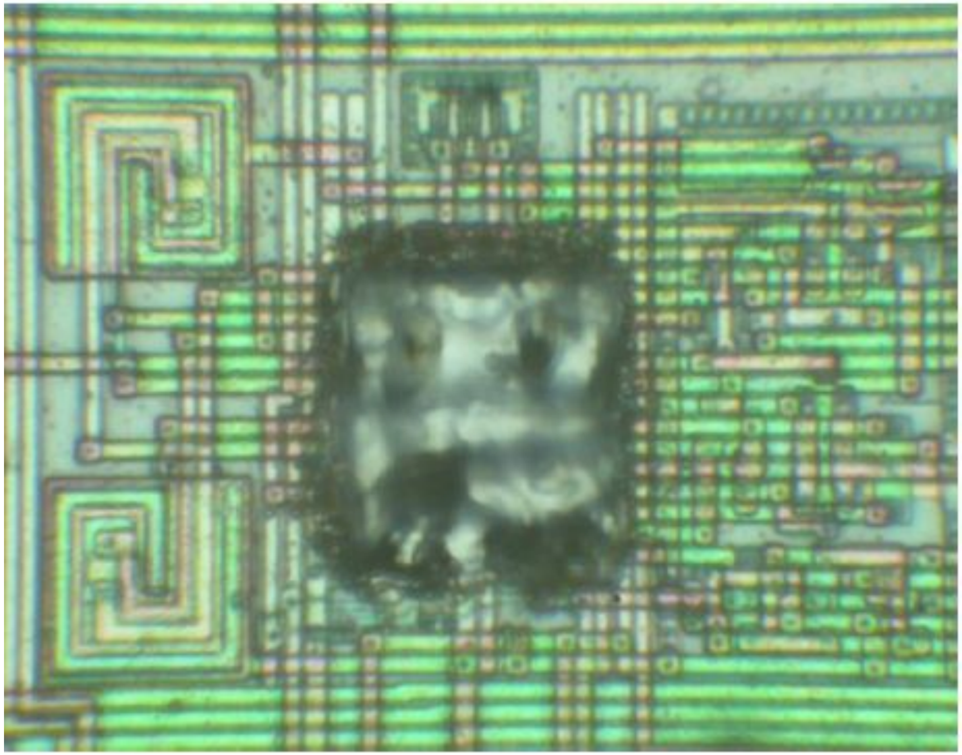


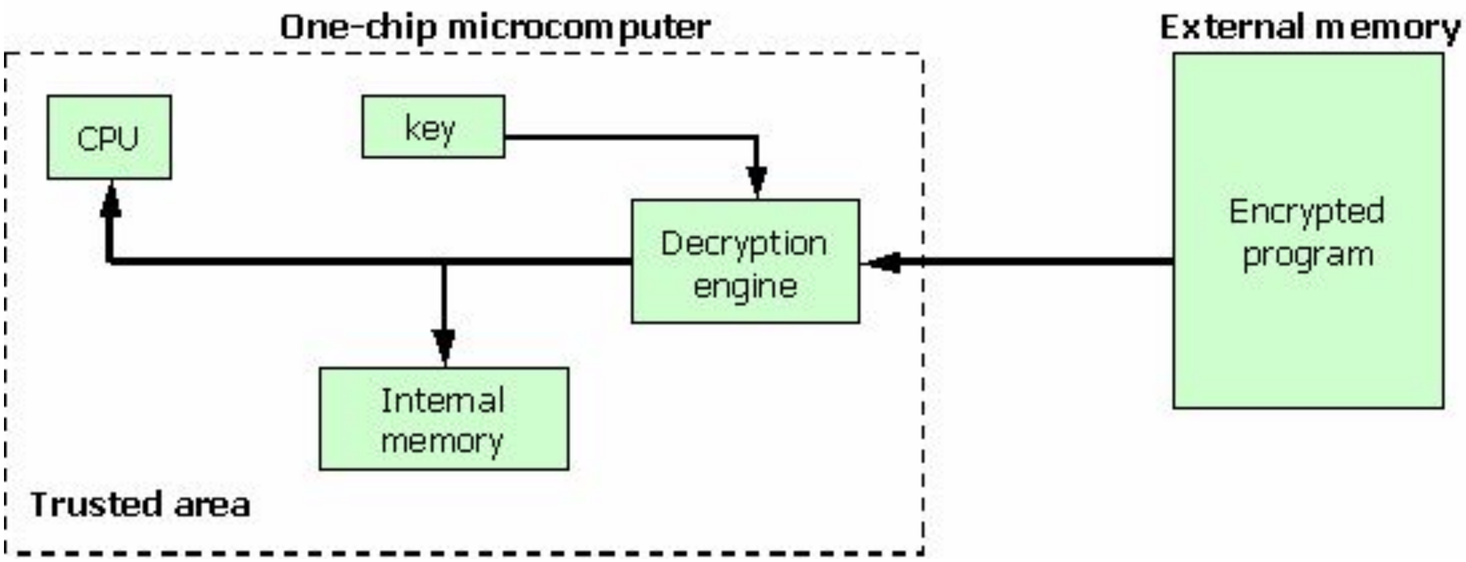
Figure 72. Disabling the security in the PIC16F628 microcontroller by destroying the fuse control circuit with a laser cutter. 500× magnification

Countermeasures

- Bus Encryption
- Top-layer Sensor Meshes
- ASICs and custom ICs
- Internal Voltage and Clock Frequency Sensors
- Light Sensor

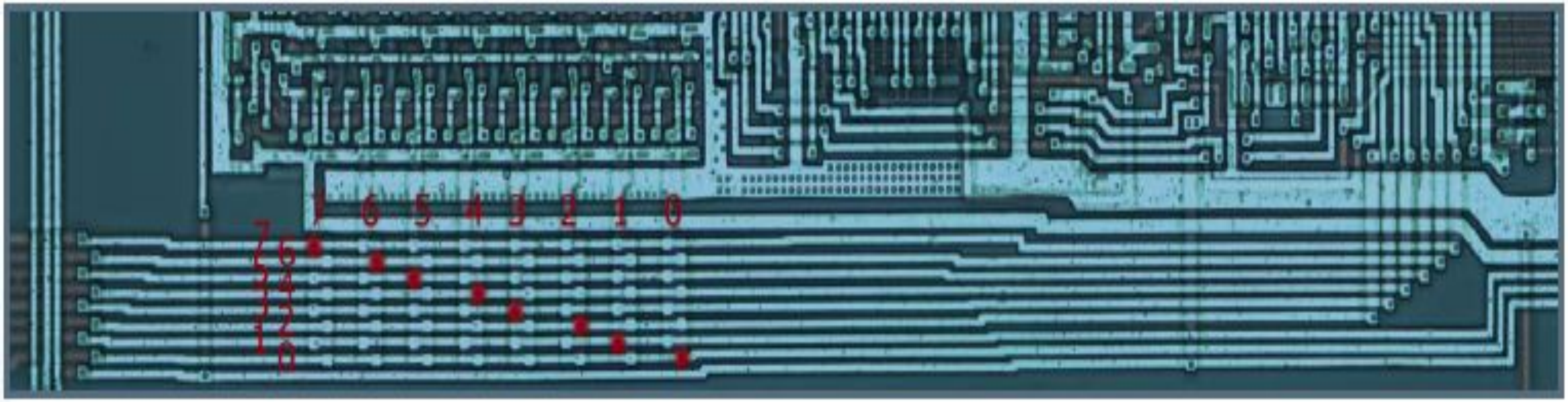
Countermeasures: Bus Encryption

- The **bus encryption** is used to protect the sensitive information from probing
  - Basically, the memory content is encrypted and then sent to the CPU by data bus
  - Before the data used in CPU, it is decrypted



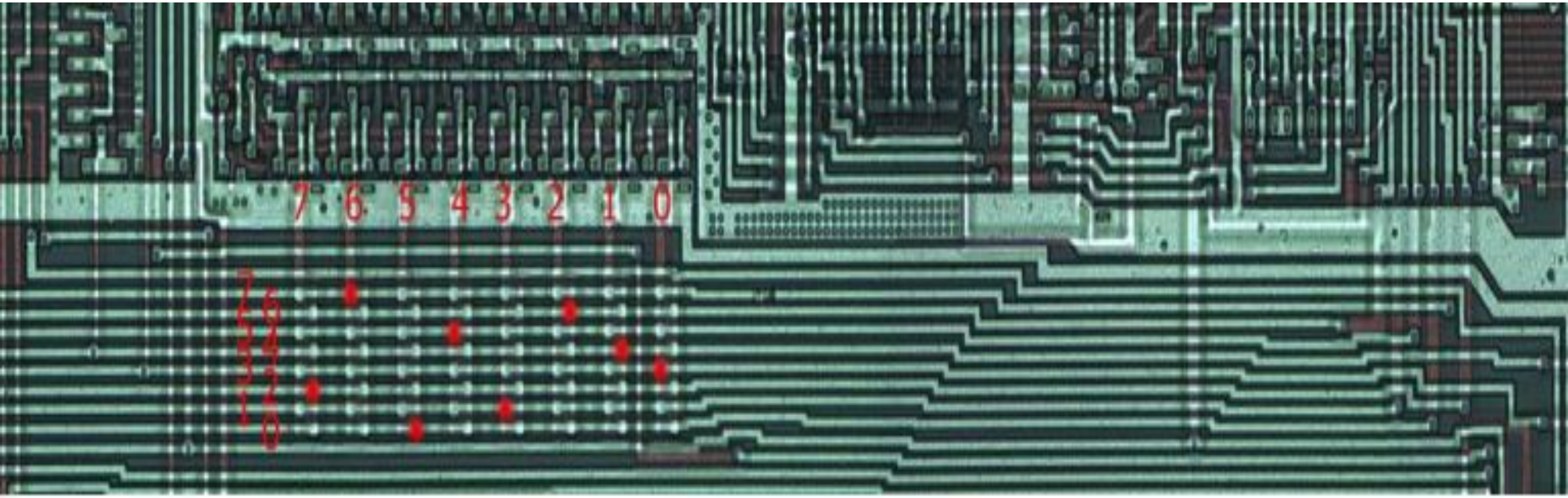
Countermeasure: Bus Scrambling

- **Typical probing areas**
  - Memory bus drivers
  - Data bus itself where lines are organized in proper CPU bus width
  - Bus order is always in order (0..7 or 7..0)

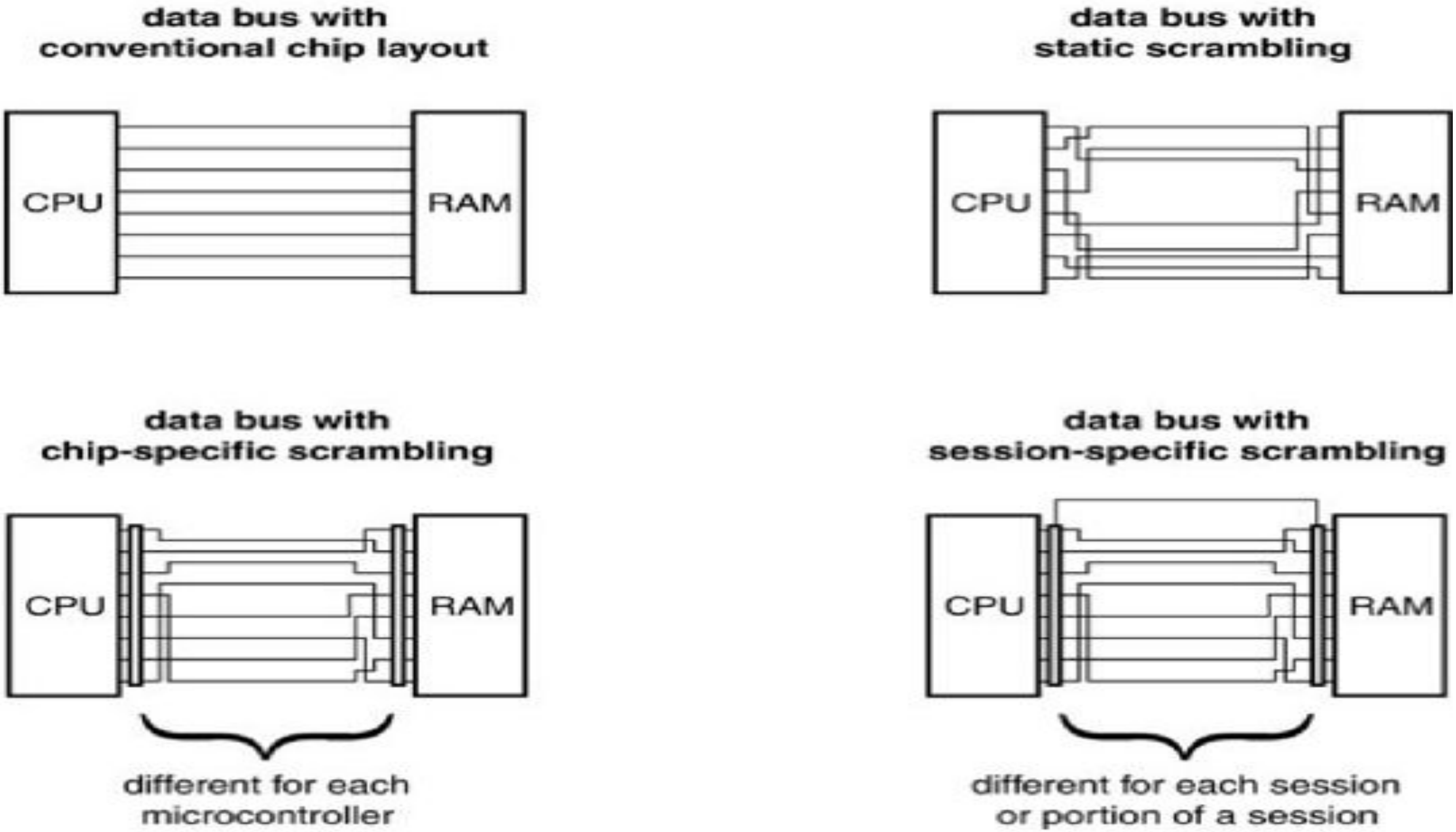


Countermeasure: Bus Scrambling

- **Data bus scrambling is used to confuse attackers**
  - Order of the data bus is changed to make it difficult to observe bus signals



Bus Scrambling



Countermeasures: Sensors

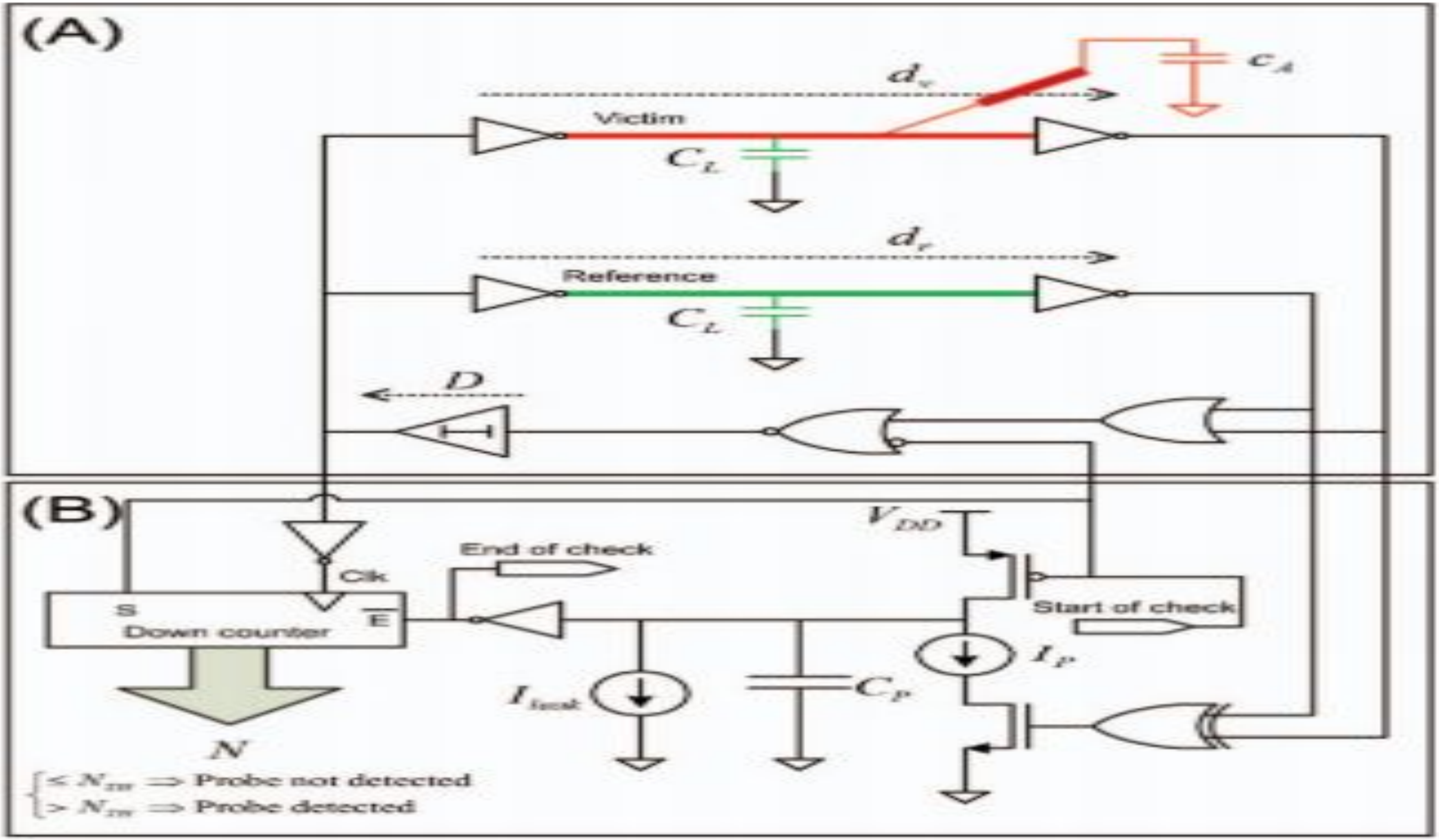
- Different kind of sensors can be used to detect attack attempt
  - Voltage and frequency sensors for glitching attacks
  - Light sensor can be helpful against decapsulation of the device

- Special purpose sensors can be created to detect probing
  - Ring oscillator based detector (Probing Attempt Detector)

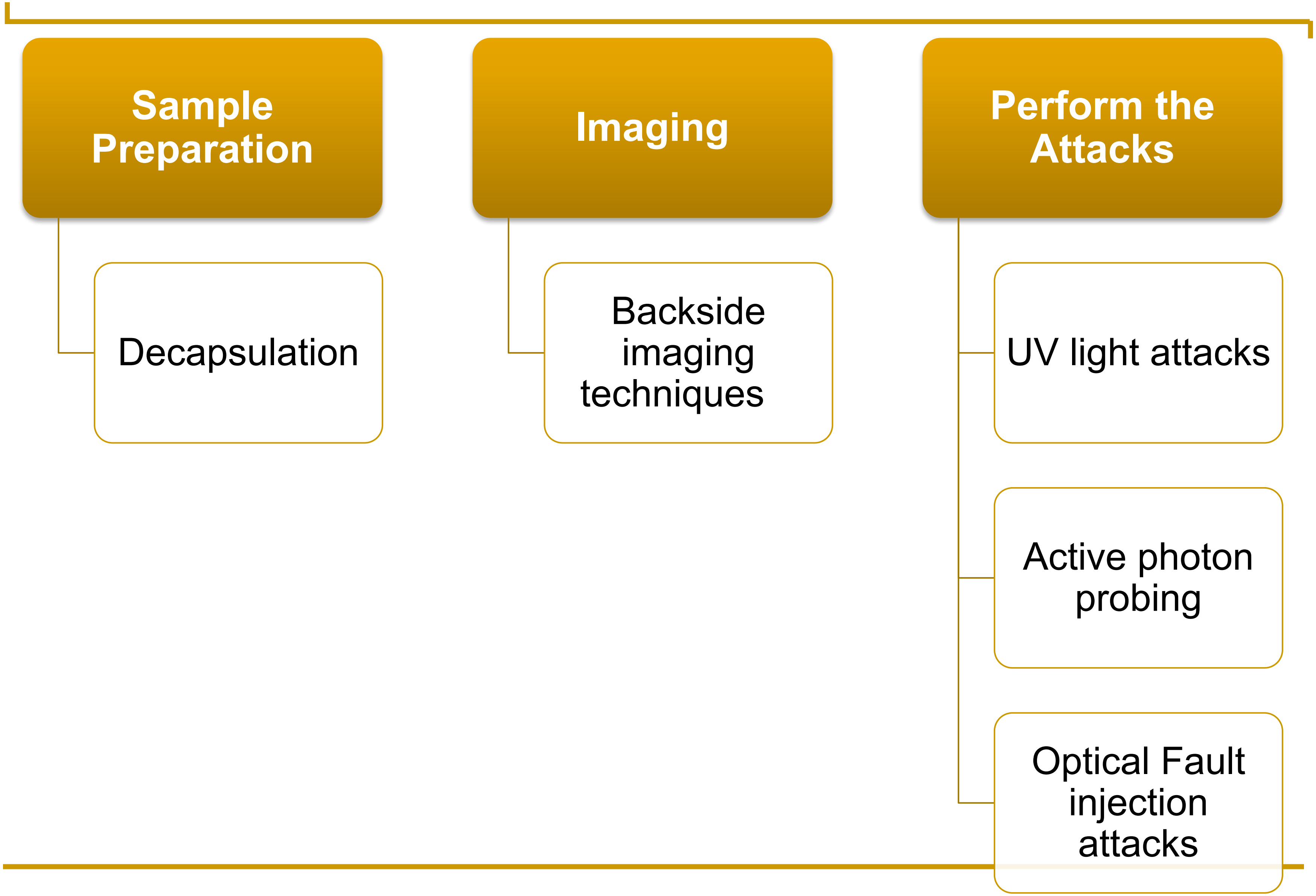
Sensors: Probing Attempt Detector (PAD)

- Exploits the fact that probing will change the capacitance in the bus line.
  - Place ring oscillators on the bus lines
  - When the probe touches the one or more bus lines, frequency of the ring oscillator changes
    - Because of the added capacitance
  - PAD observes the bus lines continuously, when they have significant difference, it sets a flag that there is a probing attempt on one of the lines

Sensors: Probing Attempt Detector



Semi-Invasive Attacks



Sample Preparation

Decapsulation

Imaging

Backside imaging techniques

Perform the Attacks

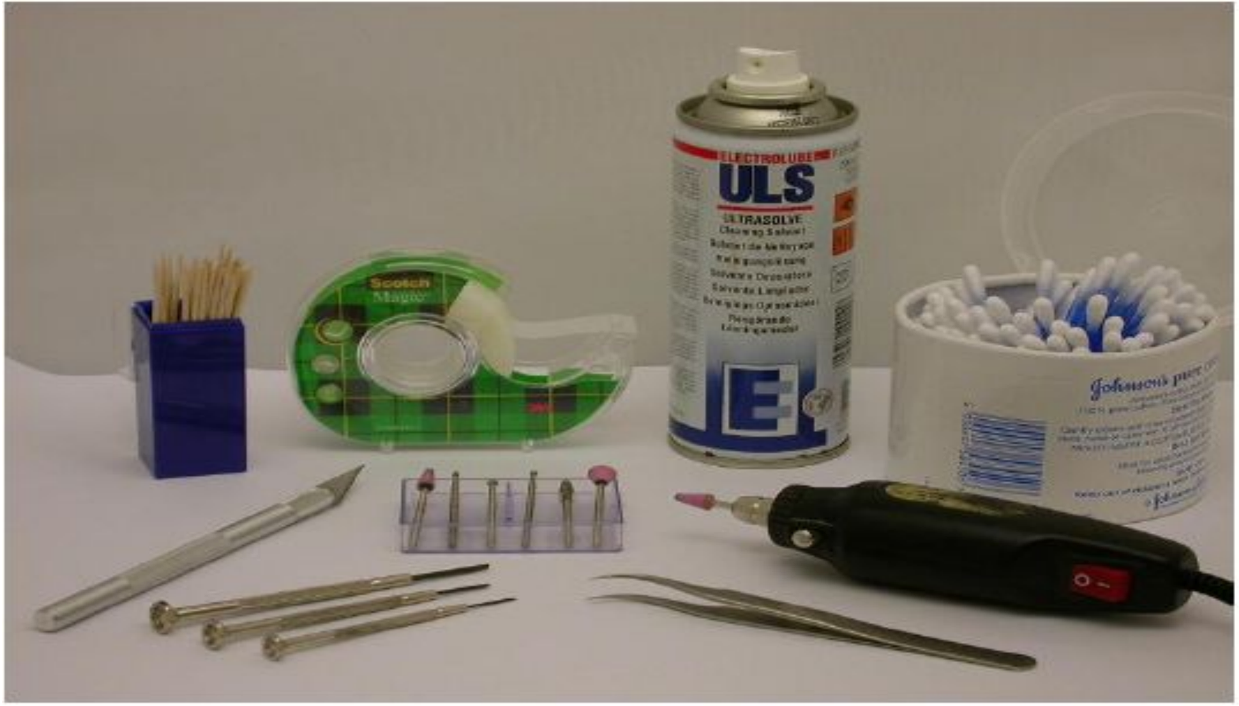
UV light attacks

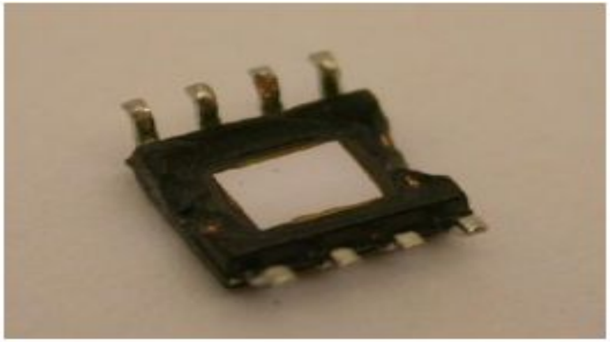
Active photon probing

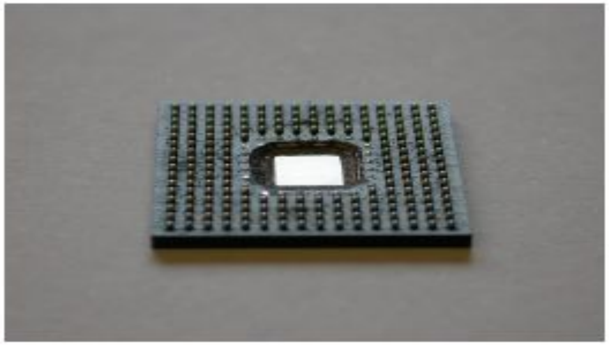
Optical Fault injection attacks

Semi-Invasive Attacks: Sample Preparation

- Decapsulation of the chip to prepare it for attacks.
- For the modern chips, backside decapsulation is used







Semi-Invasive Attacks: Imaging

- Down to 0.8 µm technology, it was possible to identify all the major elements of microcontrollers – ROM, EEPROM, SRAM, CPU
- Difficult to distinguish for newer technologies
- Can be observed with infrared light from rear side
- Backside imaging also is useful to extract the Mask ROM content

Semi-Invasive Attacks: Imaging

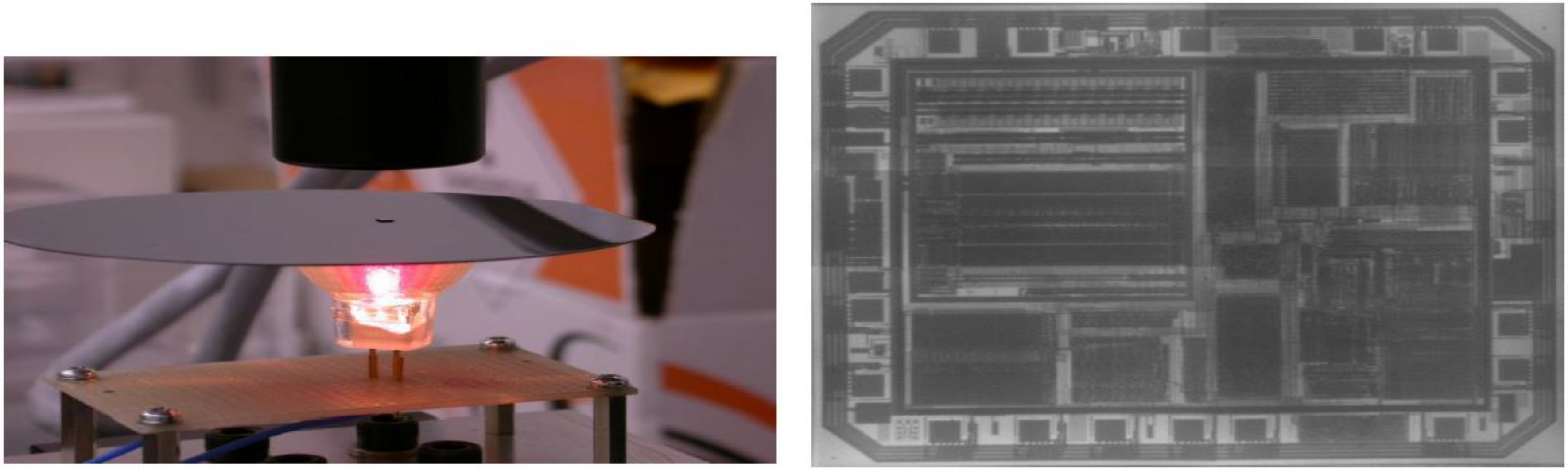


Figure 78. Transmitted light setup and image of the MSP430F112 microcontroller. 50× magnification

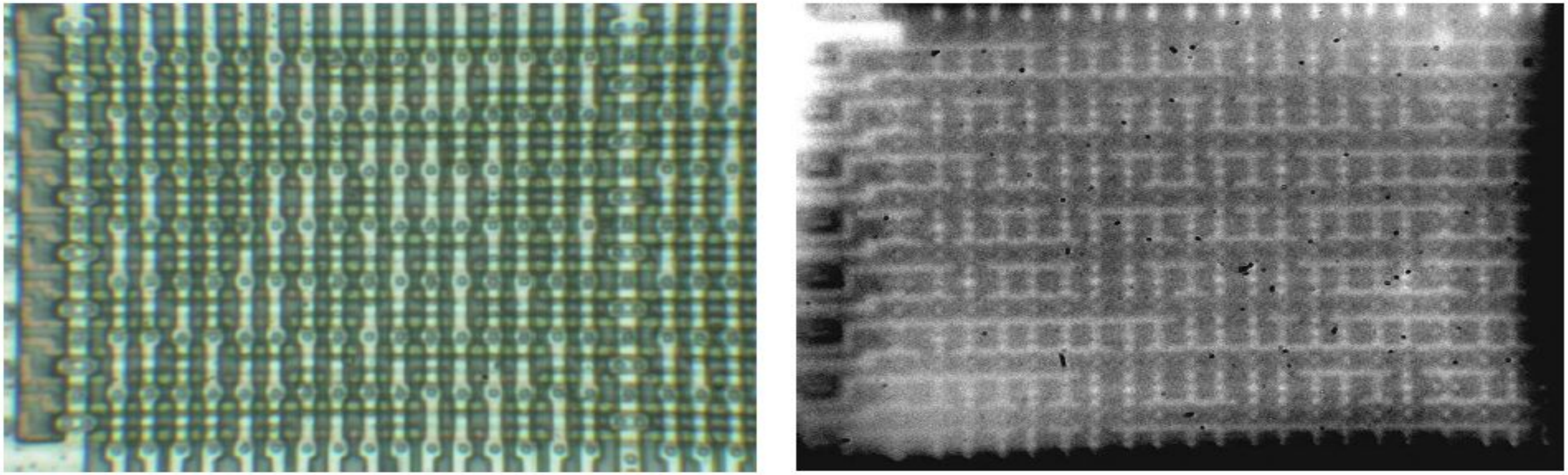
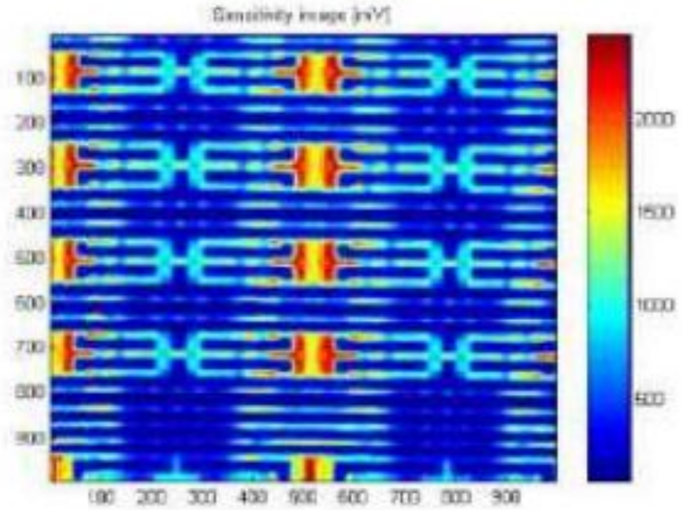


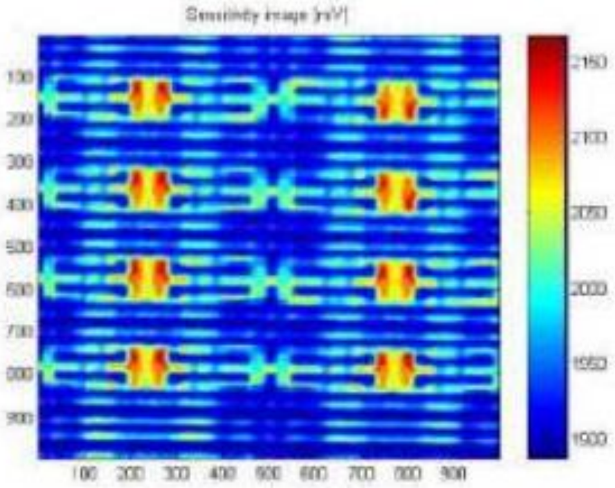
Figure 79. Standard optical image and reflected light backside image of the Mask ROM inside MC68HC705P6A microcontroller built with 1.0 μm technology. 500× magnification

Reading the Logic State of CMOS Transistors

- Red low power laser beams ionize active areas
  - Power off imaging identifies active areas
  - Power on imaging distinguishes between closed and opened transistor channels



Power off



Power on. SRAM content:
1 1 0 0
1 1 1 0
1 1 1 1
1 1 1 1

Semi-Invasive: Optical Fault Injection Attacks

- Illumination of a target transistor causes it to conduct, thereby inducing a transient fault

- Such attacks
  - Practical
  - Do not require expensive laser equipment
  - Any individual bit of SRAM in microcontroller can be set or reset

Fault injection attacks: Changing SRAM contents

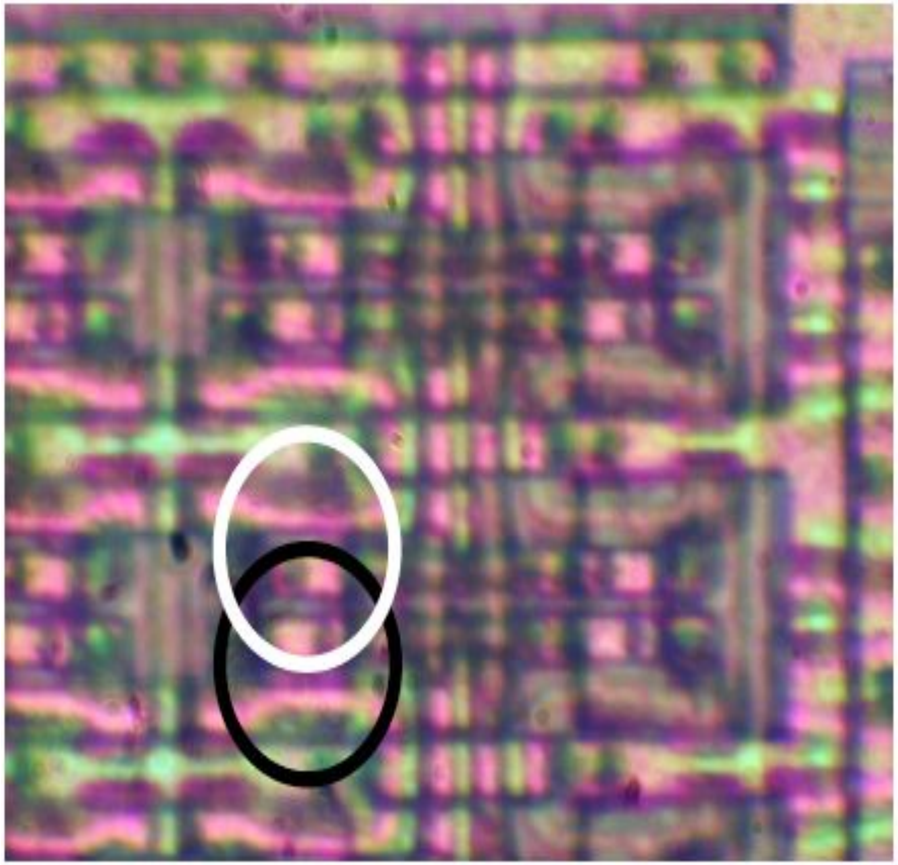


Figure 91. SRAM memory array with maximum magnification (1500×)

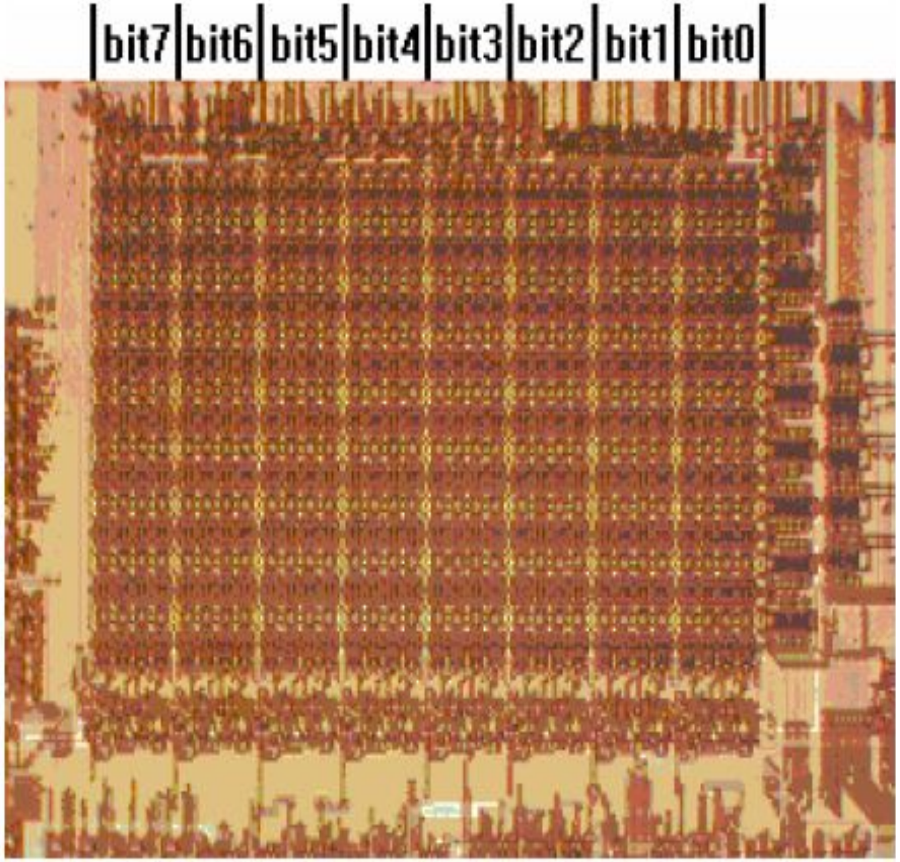


Figure 92. Allocation of data bits in SRAM memory array

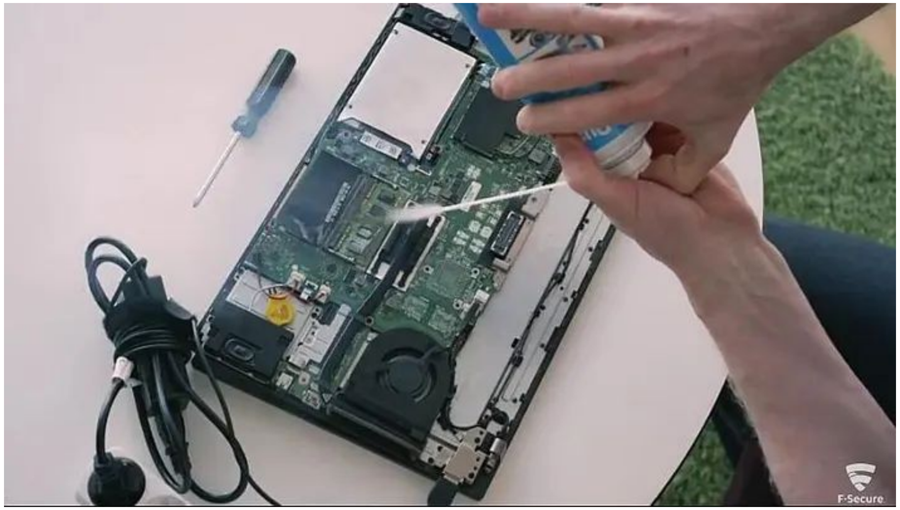
Non-volatile memory contents modification

- EPROM, EEPROM and Flash memory cells are even more sensitive to fault injection attacks.
- They can be changed by light
- This attacks can be used to disable security fuses
  - The light should be focused down to the security fuse
- These attacks do not work on modern chips built in smaller sizes

Cold Boot Attacks

A cold boot attack is a type of security vulnerability that targets data stored in the computer's RAM (Random Access Memory).

It involves restarting hardware and retrieving sensitive data (like encryption keys) from the memory before it is wiped or becomes inaccessible.

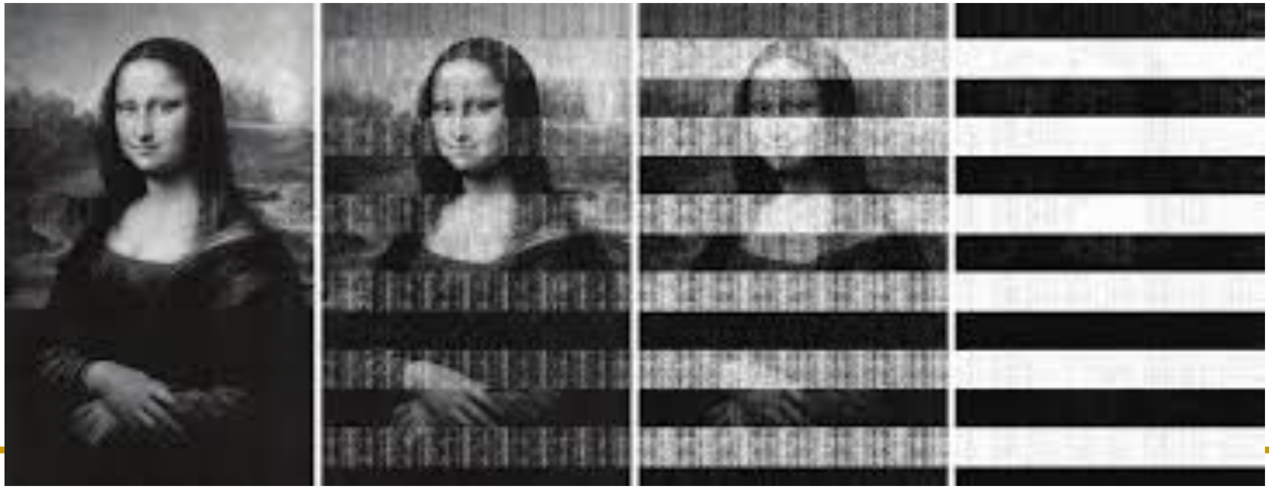


Cold Boot Attacks

Reboot the Target Device: The attacker forcibly reboots the computer to access memory that still holds sensitive information.

Extract Data from RAM: Tools or physical access are used to retrieve data from the RAM.

Use Data for Malicious Purposes: This could include extracting encryption keys, passwords, state, or other confidential information.



Cold Boot Attacks

Memory Retention:

Even after the computer is powered off, the data in the RAM can persist for several seconds to minutes before being lost.

Volatile Memory:

Memory (RAM, Flops, etc) is volatile, meaning it needs constant power to retain data. However, data can remain accessible temporarily after power loss.

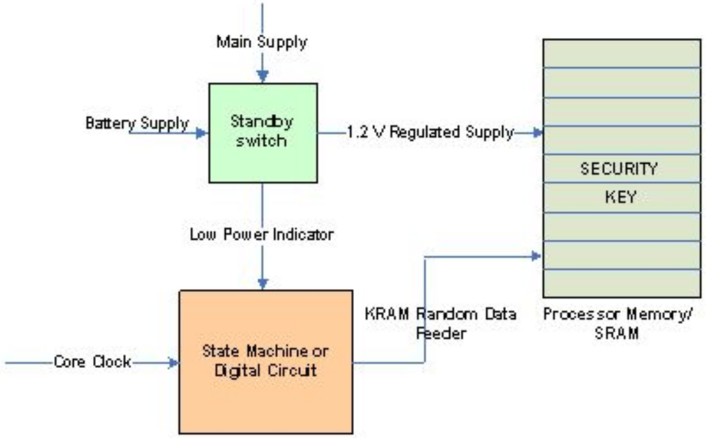
Data Remanence Effect: Residual presence of data that remains on a storage device even after it has been deleted, erased, or when power is removed

- Electron Decay is not instant. It takes time for electrons to discharge from the Integrated Circuit. What if you read it back before it is fully discharged?

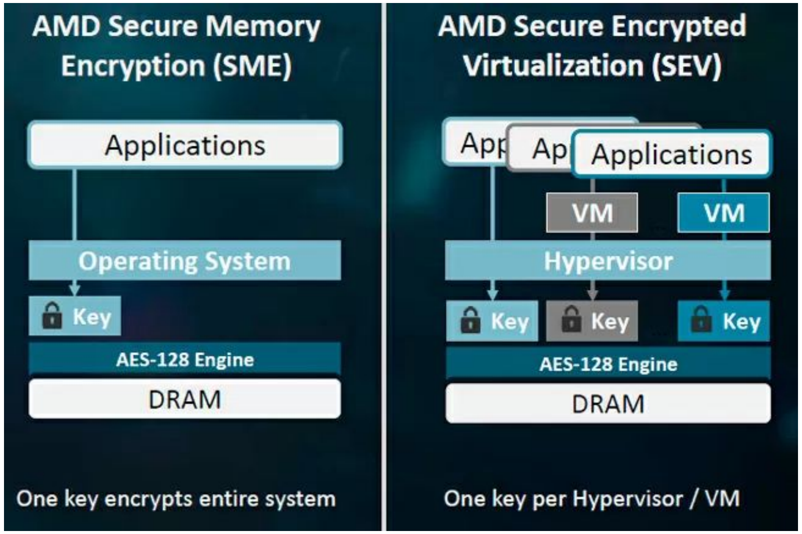
Cold Boot Attacks

Defences:

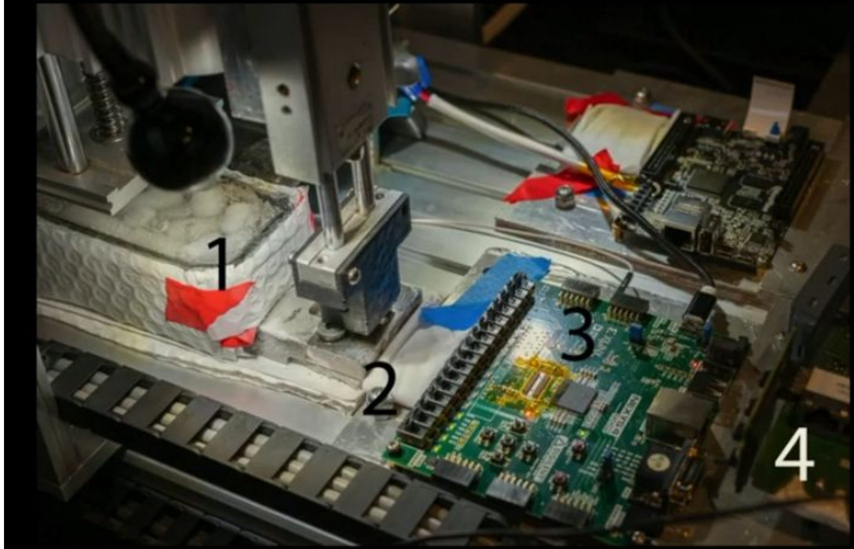
1. Randomization Architecture - circuit that pumps entropy into stateful logic (RAM, FFs) when a power cycle is detected.

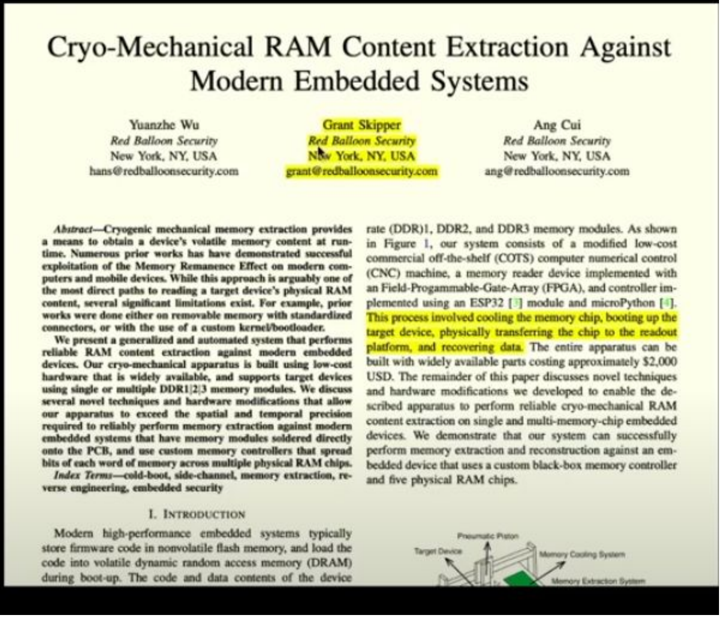


2. Direct Memory Encryption.


AMD Secure Memory Encryption (SME)
Applications
Operating System
Key
AES-128 Engine
DRAM
One key encrypts entire system
AMD Secure Encrypted Virtualization (SEV)
App
Ap
Applications
VM
VM
Hypervisor
Key
Key
Key
AES-128 Engine
DRAM
One key per Hypervisor / VM

Cold Boot Attacks





Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems

Yuanzhe Wu
Red Balloon Security
New York, NY, USA
hans@redballoonsecurity.com

Grant Skipper
Red Balloon Security
New York, NY, USA
grant@redballoonsecurity.com

Ang Cui
Red Balloon Security
New York, NY, USA
ang@redballoonsecurity.com

***Abstract*—Cryogenic mechanical memory extraction provides a means to obtain a device's volatile memory content at runtime. Numerous prior works has have demonstrated successful exploitation of the Memory Remanence Effect on modern computers and mobile devices. While this approach is arguably one of the most direct paths to reading a target device's physical RAM content, several significant limitations exist. For example, prior works were done either on removable memory with standardized connectors, or with the use of a custom kernel/bootloader.**

We present a generalized and automated system that performs reliable RAM content extraction against modern embedded devices. Our cryo-mechanical apparatus is built using low-cost hardware that is widely available, and supports target devices using single or multiple DDR1|2|3 memory modules. We discuss several novel techniques and hardware modifications that allow our apparatus to exceed the spatial and temporal precision required to reliably perform memory extraction against modern embedded systems that have memory modules soldered directly onto the PCB, and use custom memory controllers that spread bits of each word of memory across multiple physical RAM chips.

***Index Terms*—cold-boot, side-channel, memory extraction, reverse engineering, embedded security**

I. Introduction

Modern high-performance embedded systems typically store firmware code in nonvolatile flash memory, and load the code into volatile dynamic random access memory (DRAM) during boot-up. The code and data contents of the device

rate (DDR)1, DDR2, and DDR3 memory modules. As shown in Figure 1, our system consists of a modified low-cost commercial off-the-shelf (COTS) computer numerical control (CNC) machine, a memory reader device implemented with an Field-Progammable-Gate-Array (FPGA), and controller implemented using an ESP32 [3] module and microPython [4]. This process involved cooling the memory chip, booting up the target device, physically transferring the chip to the readout platform, and recovering data. The entire apparatus can be built with widely available parts costing approximately $2,000 USD. The remainder of this paper discusses novel techniques and hardware modifications we developed to enable the described apparatus to perform reliable cryo-mechanical RAM content extraction on single and multi-memory-chip embedded devices. We demonstrate that our system can successfully perform memory extraction and reconstruction against an embedded device that uses a custom black-box memory controller and five physical RAM chips.

https://www.youtube.com/watch?v=nTvIQDe0rQU

References

- Semi-invasive attacks A new approach to hardware security analysis, *Sergei P. Skorobogatov*
- Physical Attacks and Tamper Resistance *Sergei Skorobogatov*
- Hardware Engines for Bus Encryption: a Survey of Existing Techniques *R. Elbaz, L. Torres, G. Sassatelli,* P. Guillemin, C. Anguille and C. Buatois, J. B. Rigaud
- Wet and Dry Etching *Avinash P. Nayak Logeeswaran VJ and M. Saif Islam*
- Security Failures in Secure Devices, *Christopher Tarnovsky Black Hat, DC*

References

- *www.flylogic.net/blog*
- http://www.siliconzoo.org/
- Smart Card Handbook, *by Wolgang Ranki, Wolfgang Effing*
- Detection of Probing Attempts in Secure ICs, *Salvador Manich, Markus S. Wamser and Georg Sigl*