Chapter 10

Physical Attacks and Countermeasures

Russia Shoots Down Its Own Secret Drone Over Ukraine!

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	Active

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

- **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

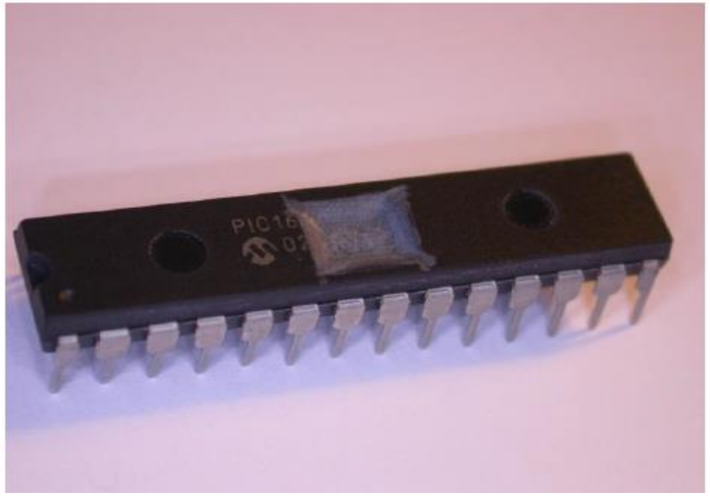
Exposing the chip package to acid

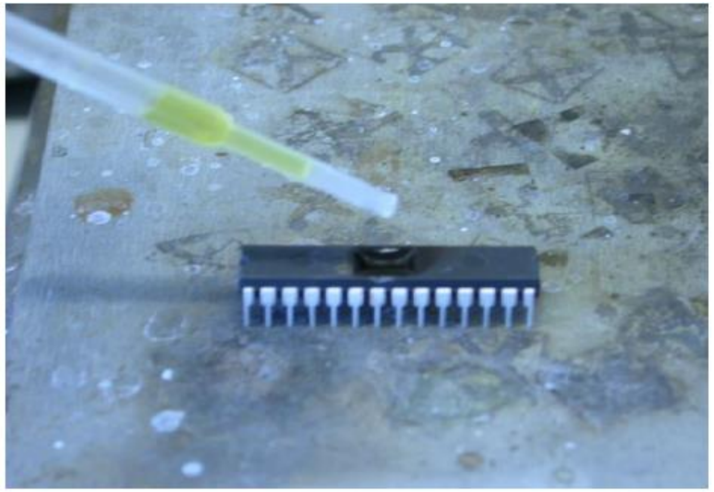
- Fuming Nitric Acid or mixture of Fuming Nitric Acid and concentrated Sulphuric Acid can be used
- The acid is applied with a pipette to the hole in the chip, it should be preheated to 50-70 °C

Cleaning the chip from the reaction products

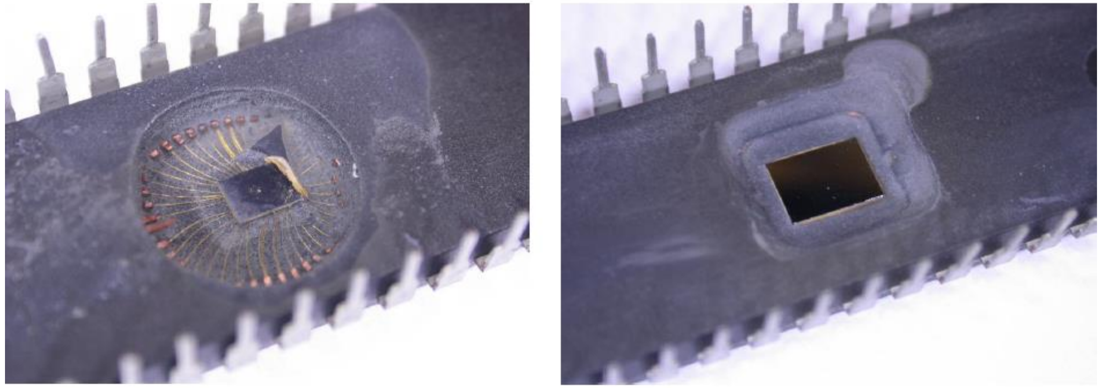
- After 10-30 second, the chip is sprayed with dry acetone several times
- Also, ultrasonic bath can be used to clean the chip die surface

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

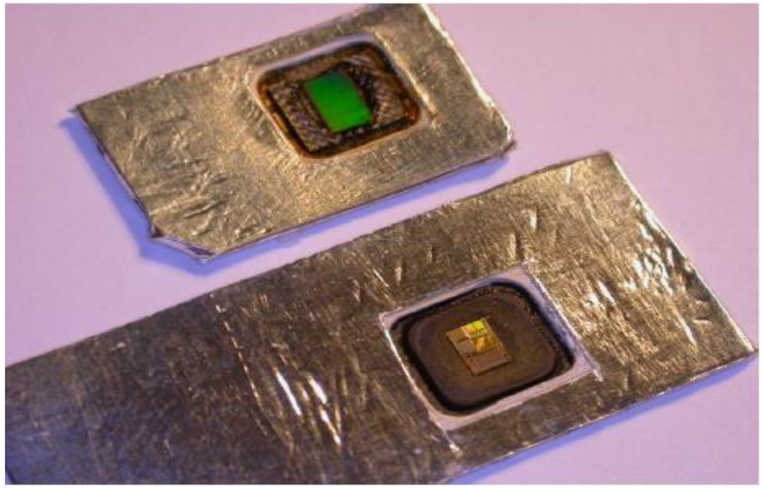
For large quantities, automated decapsulation systems can be used.

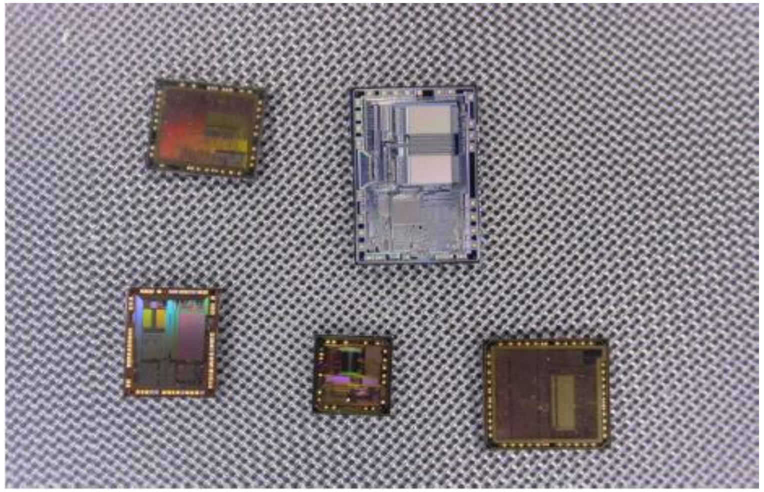
- Very little skill and experience is required to operate it
- Cost around $15,000
- Also, they consume ten times more acid than the manual decapsulation, so the disposal of the waste should be done in proper way

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





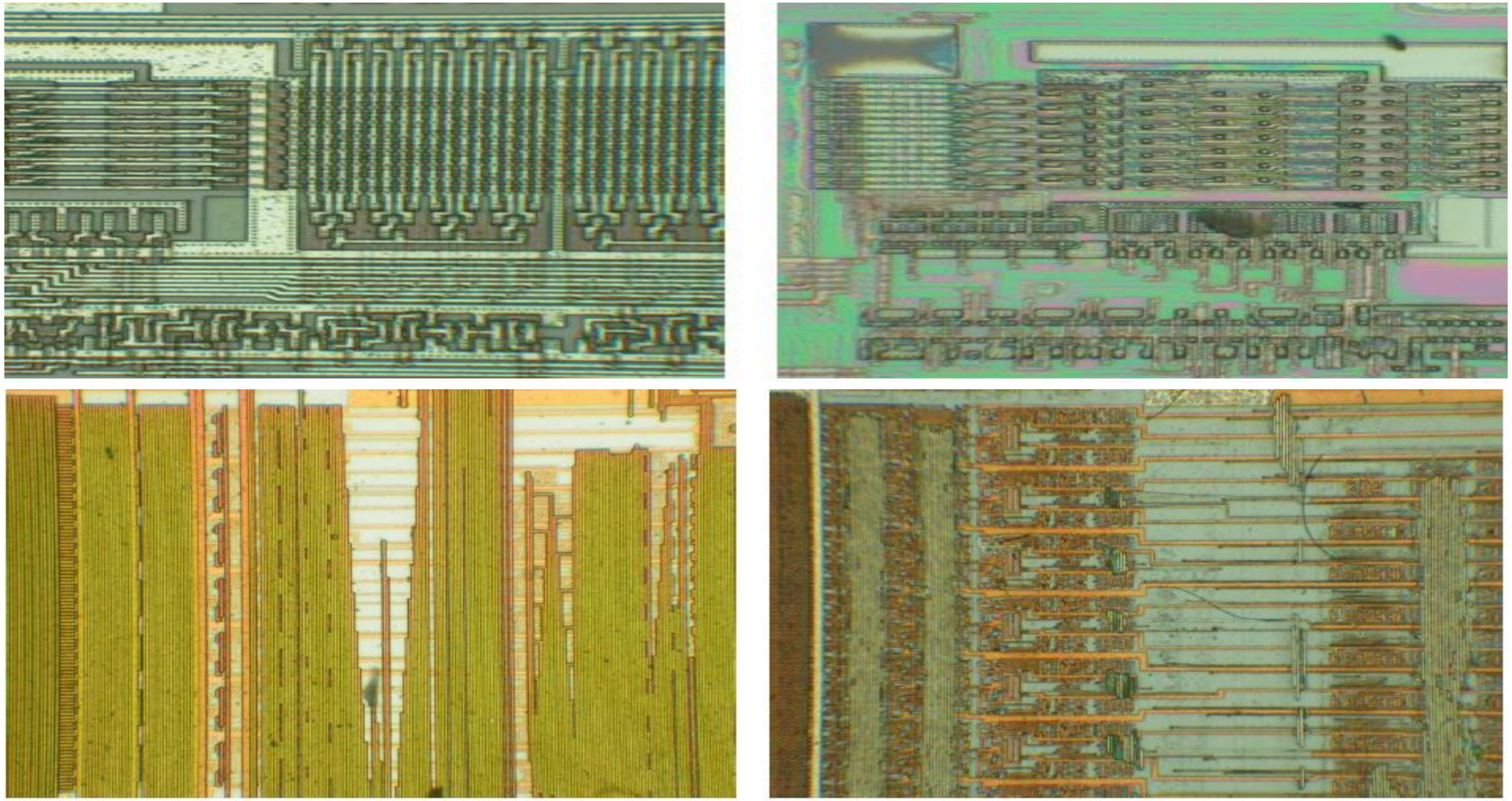
Sample Preparation

- **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.

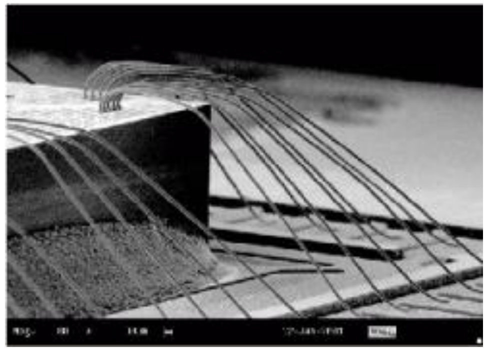
Deprocessing



Top: Motorola MC68HC705C9A microcontroller. The metal layer is removed exposing the polysilicon and the doping layers.
Bottom: Microchip PIC16F76 microcontroller. The top metal layer is removed exposing the second metal layer.

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

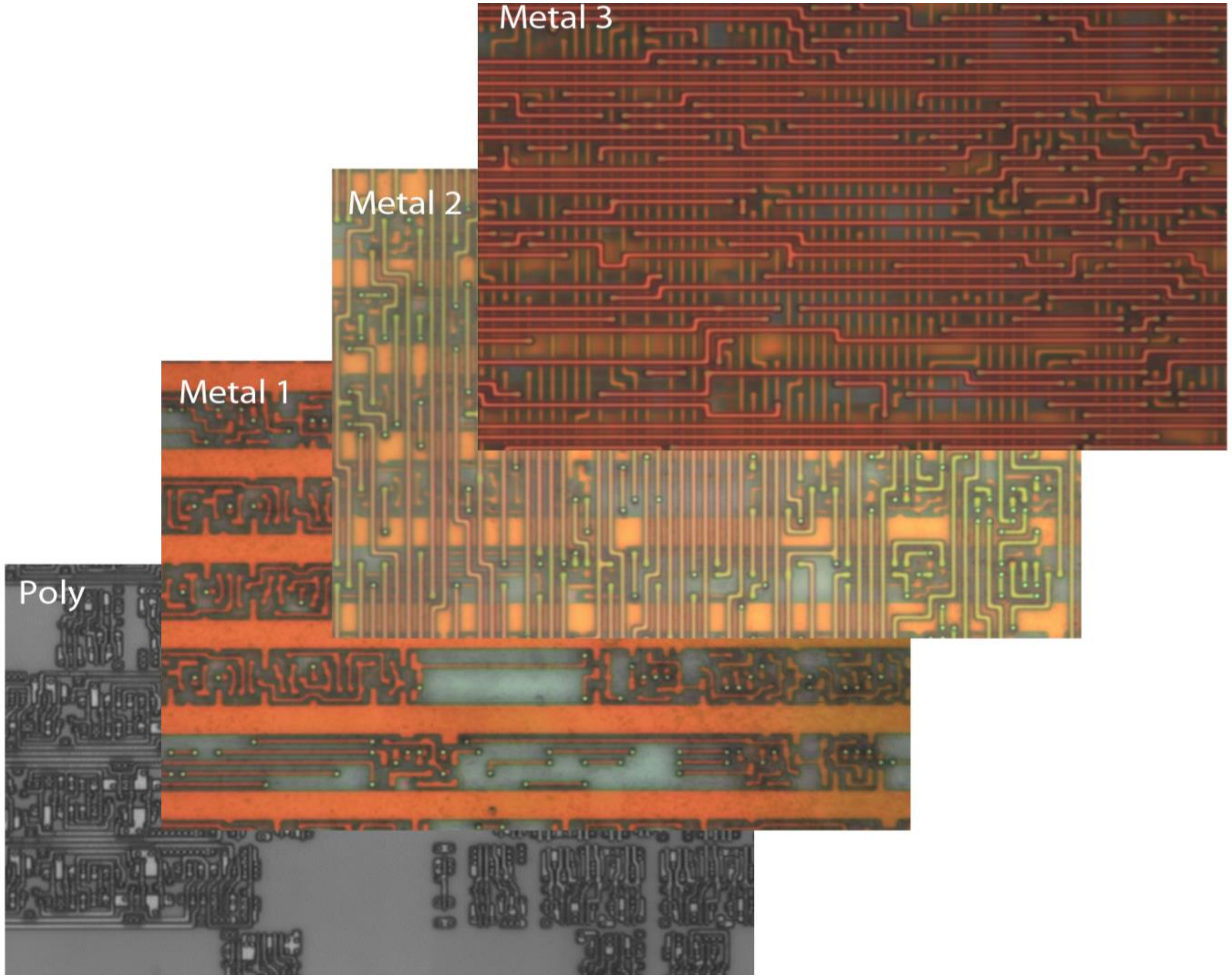
- It is tedious and time-consuming process
- For the smartcards and microcontrollers, both **structural** and **program-code** reverse engineering is required.
  - First, security protection should be understood by **partial reverse engineering**
  - If memory bus encryption was used, the hardware responsible 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

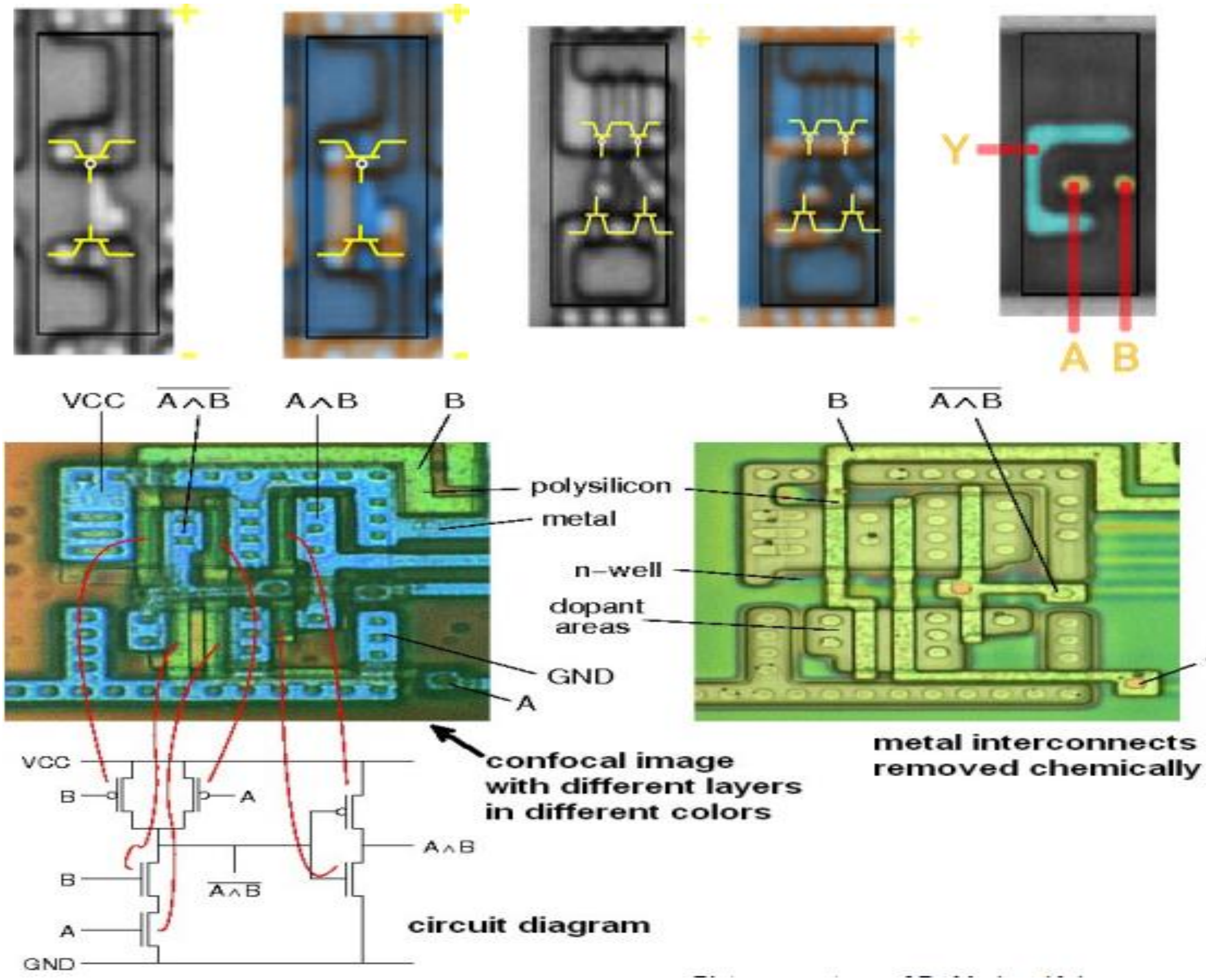
- **Optical Imaging:**
  - For reverse engineering the silicon chips down to 0.18 µm feature size, an optical microscope with a digital camera can be used

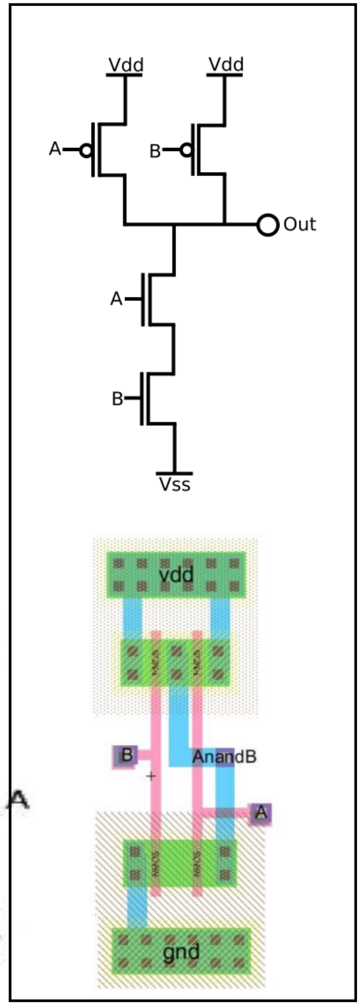
- **Scanning Electron Microscopy (SEM):**
  - For semiconductor chips fabricated with 0.13 µm or smaller technology, images are created using a SEM which has a resolution better than 10 nm.

Layer by Layer Imaging



Reverse Engineering





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

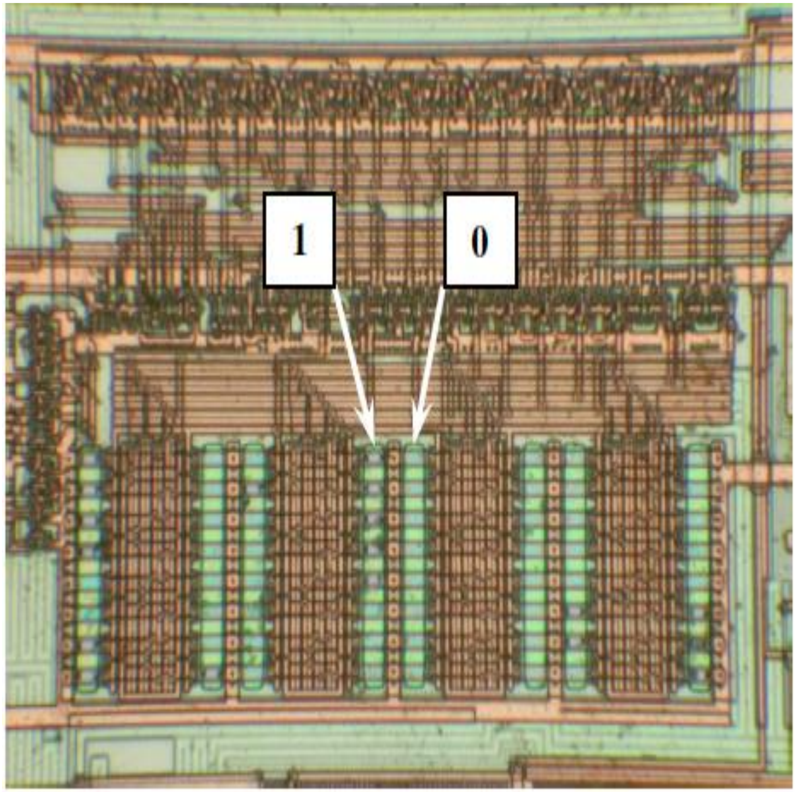


Figure 17. Laser ROM in Dallas DS1961S iButton chip [49]. Information can be read optically and altered with a laser cutter

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.

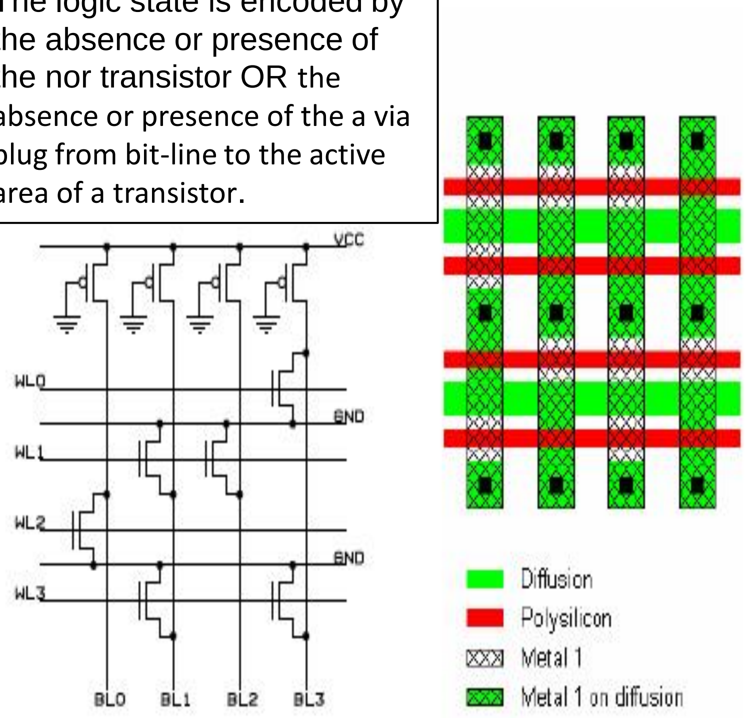


Figure 18. Configuration and layout of MOS NOR ROM with active layer programming. This type of memory can be read optically

Reverse Engineering

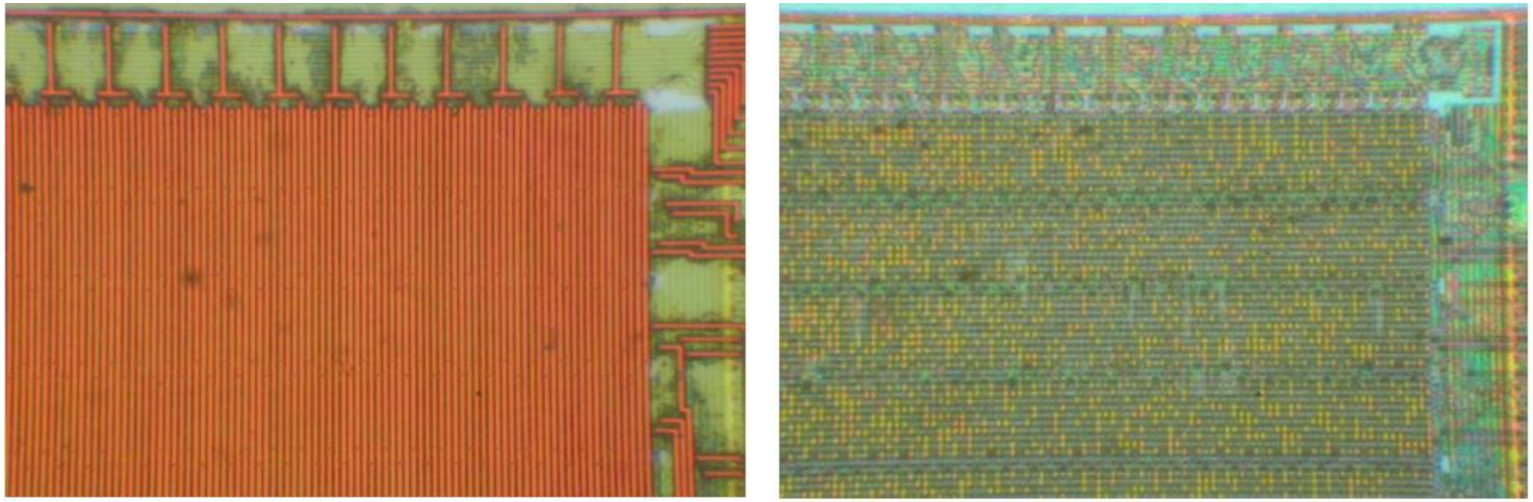


Figure 61. Optical image of the Mask ROM inside μPD78F9116 microcontroller before and after wet chemical etching. 500× magnification

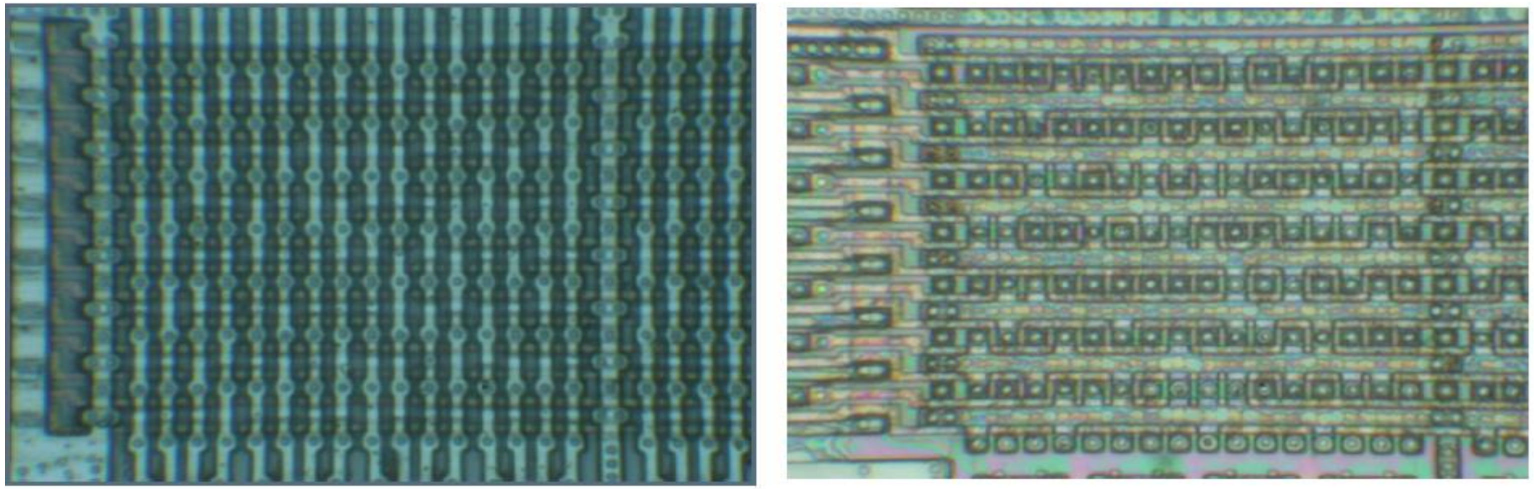


Figure 60. Optical image of the Mask ROM inside MC68HC705C9A microcontroller before and after wet chemical etching. 500× magnification

Reverse Engineering

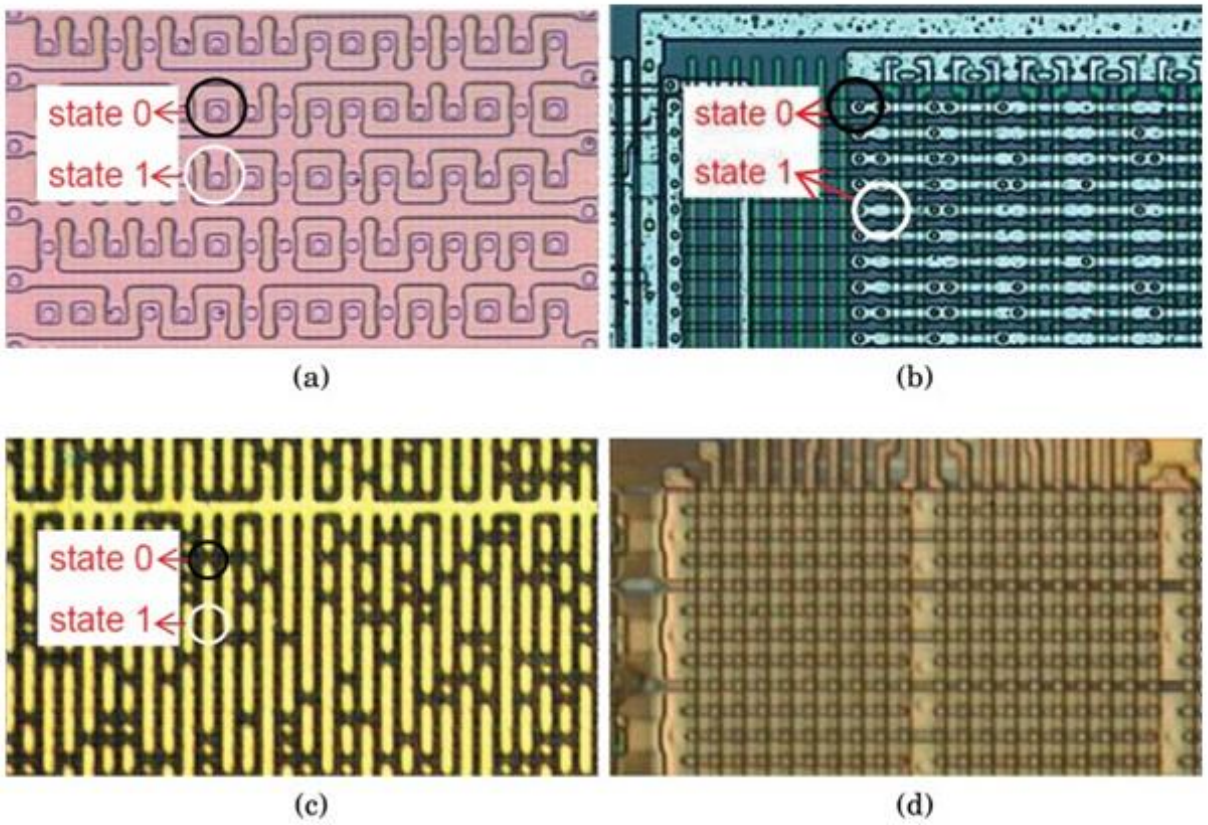


Figure 16: Optical inspection of active-layer programming ROM [63](a), contact- layer programming ROM [28] (b), metal-layer programming ROM [64](c), and implant programming ROM before selective etch [64](d).

Reverse Engineering

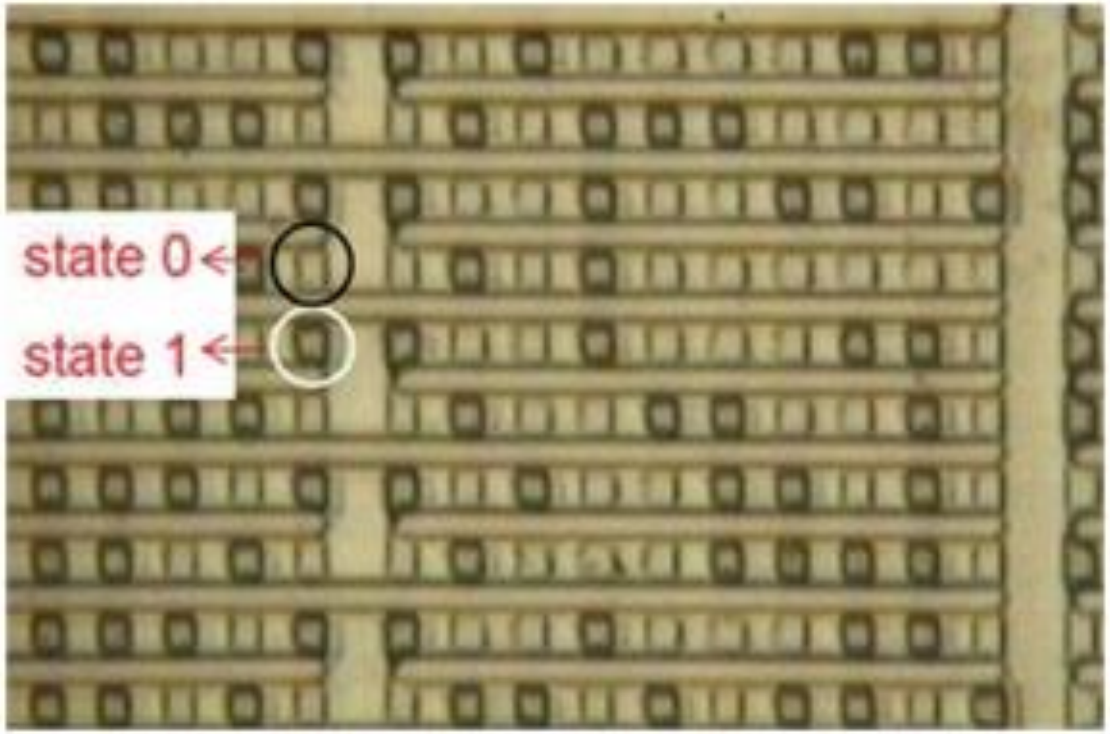


Figure 17: Optical inspection of implant programming ROM after selective etch [64].

Invasive Attacks: Microprobing

- **Microprobing**
  - Could be used for both *Confidentiality* and *Integrity* violationseavesdropping 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
- Usually to extract the information such as memory contents or a secret key, microprobing is applied to the internal CPU data bus. Generally, it is difficult to observe whole data bus at a time.
- Memory extraction from smartcards is more difficult because their software generally does not allow to access to the internal memory. So, it is required to exploit some CPU components such as an address counter or instruction decoder to access all the memory cells.

Microprobing

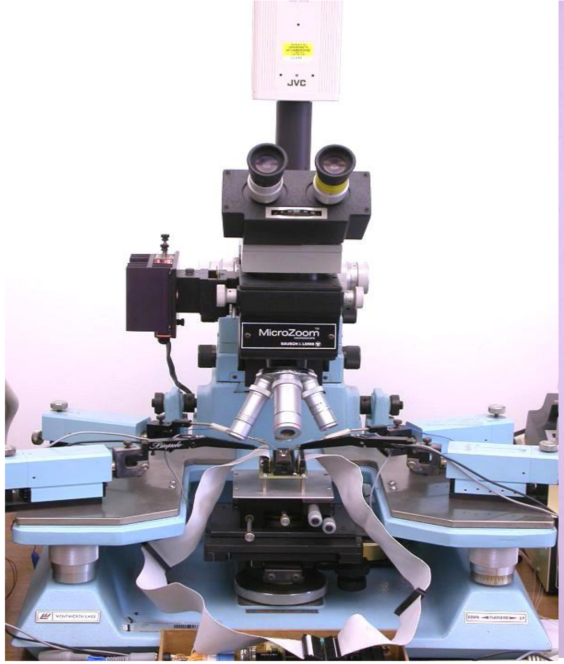
- The most important tool for microprobing attacks is microprobing station which consist of a microscope, stage, device test socket, micromanipulators and probe tips. By the means of microscope, attacker sees the internal structure of the chip and using micromanipulator and microscope, attacker moves a probe tip with submicron precision to the desired signal wire.

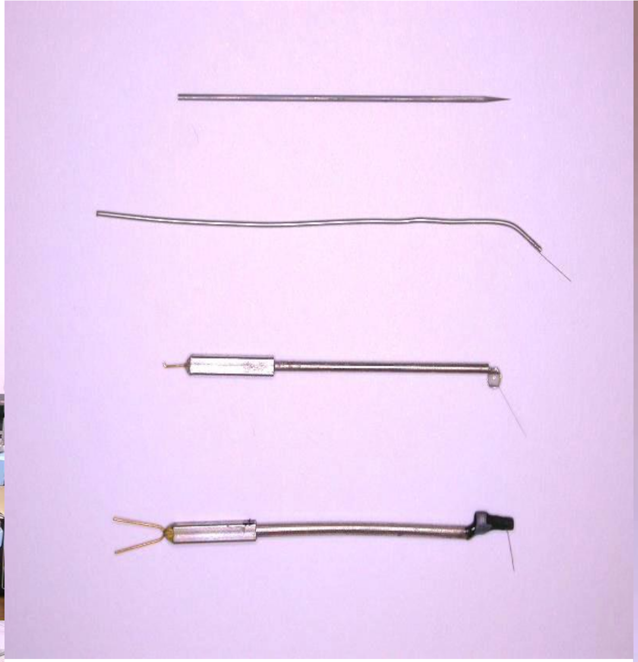
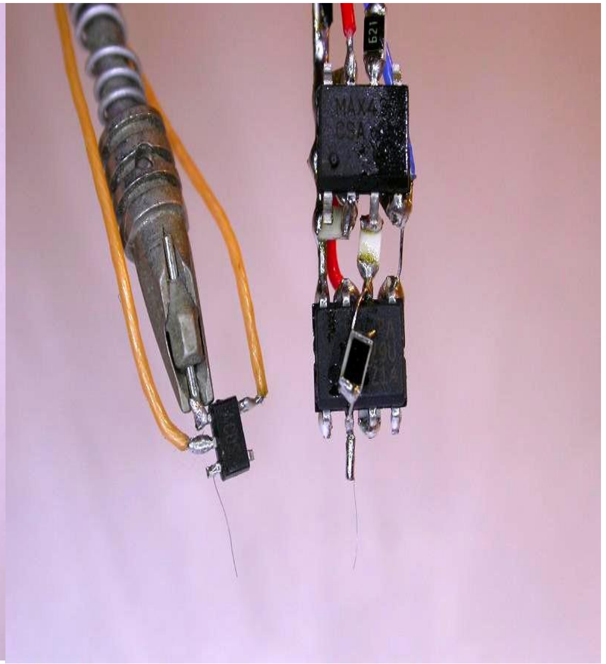
- The probe tip can be either passive or active. Passive tips can be used for both eavesdropping and injecting signals. They are directly connected to the oscilloscope so that they have low impedance and high capacitance. Therefore, they can not be used to observe any other signal rather than data bus which are buffered usually.
- Active probe tips has a FET amplifier close to the end of the tip. They have low capacitance and high impedance.

- The stage under microscope is used to position the test socket 1um precision is enough for it.

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.



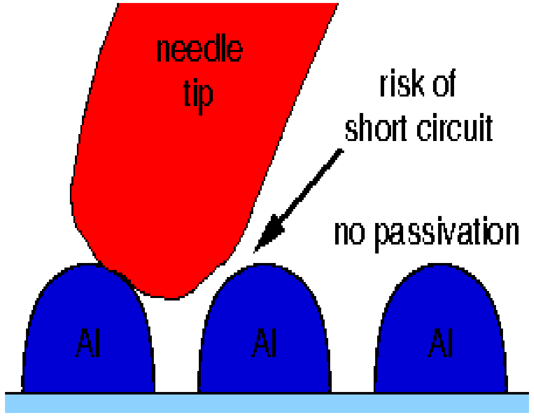
Invasive Attacks: Microprobing

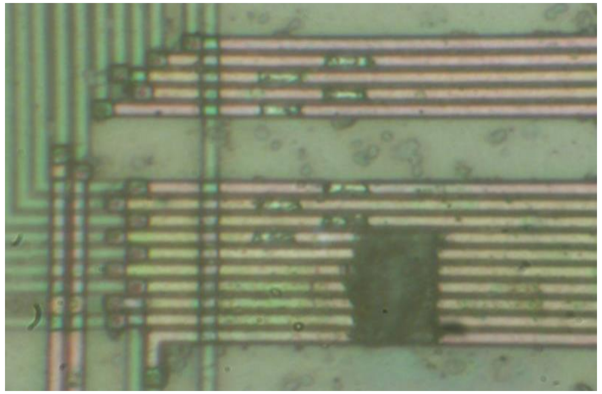
- **Microprobing is applied to the internal CPU data bus**
  - Difficult to observe whole data bus all at once
  - There are limited number of probes
  - Two to four probes are used to observe data signals which are combined as a whole data trace later.

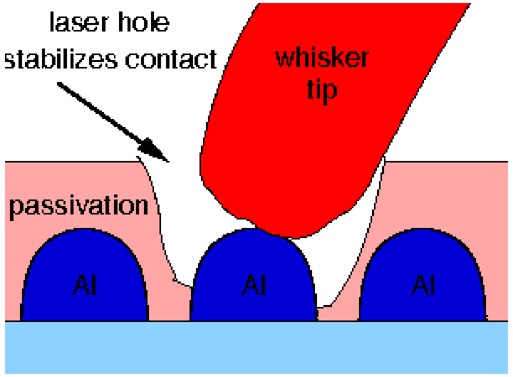
Microprobing: Laser Cutting

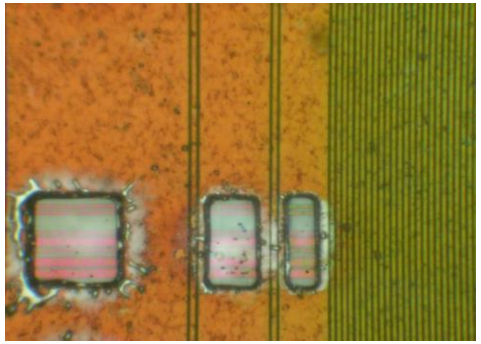
- It is used to remove passivation layer to observe the metal layer
- Laser Cutting Systems consist of:
  - laser head mounted on camera port of a microscope
  - submicron-precision stage to move the sample
- Carefully dosed laser flashes remove patches of the passivation layer with micrometer precision

Microprobing: Laser Cutting









If we remove the whole passivation layer, because the internal wires are so small there is big chance to have short circuit while microprobing.
Not to have short circuit, laser cutter used to cut the desired area on the chip to get access to the wires that we want to listen.

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 is used for the devices which are fabricated with 0.5um or smaller technologies.

FIB Workstation

- Upper left image shows a hole that is milled by FIB work station. You can create really tiny holes on the chip die with FIB.
- Upper right image shows wire cutting with FIB. It can be used chip modification attacks to disable the security circuitry.
- Lower left image shows test points created by FIB. Without removing any layer, by creating test point over the chip surface, probing attacks can be performed.
- Lower right image is an image created by FIB.

FIB Workstation

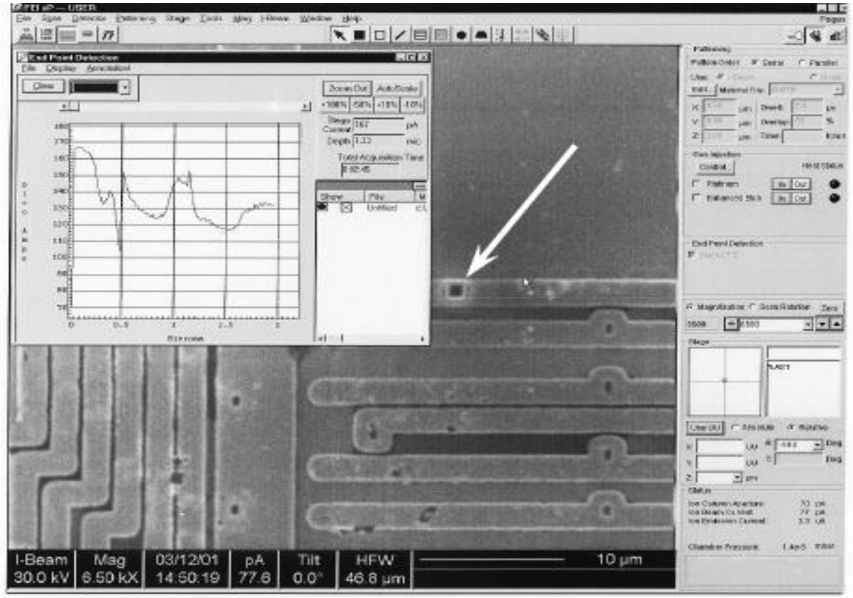


Figure 68. The process of milling the hole using FIB

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

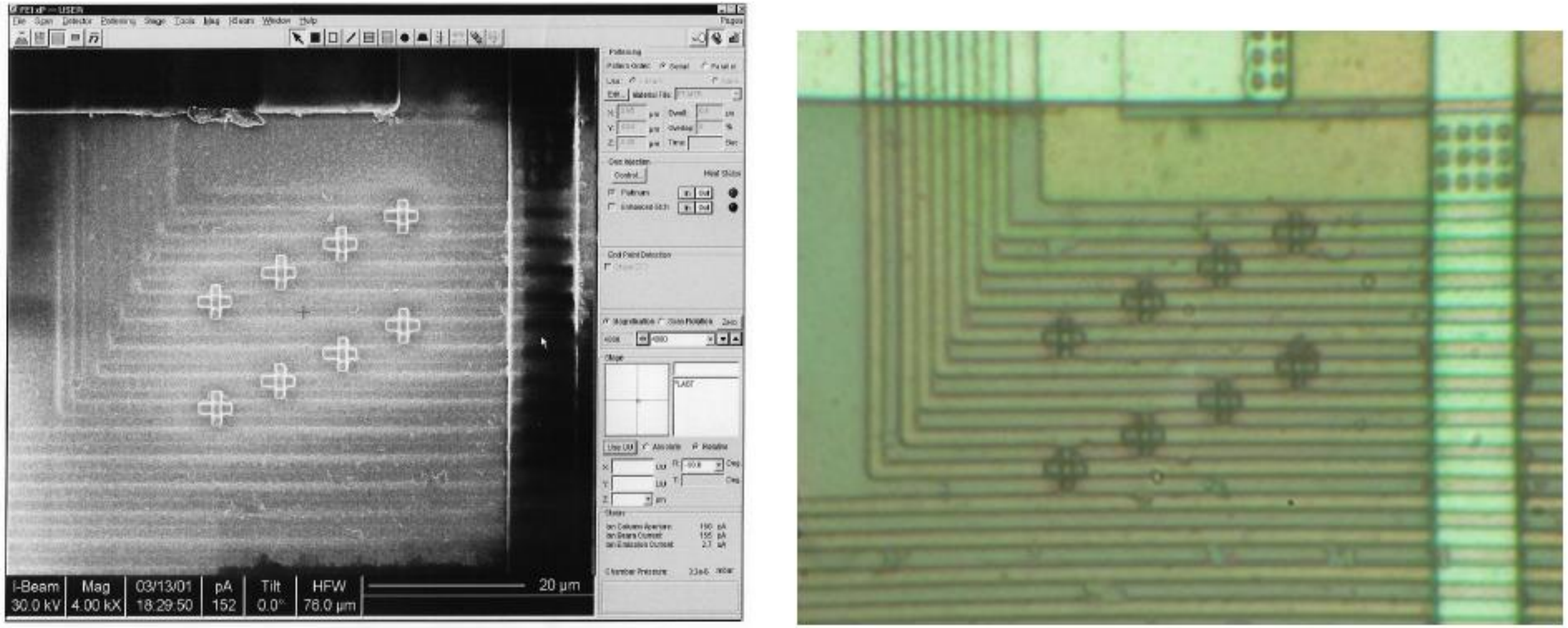


Figure 70. Test points created under FIB and optical image of these points

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

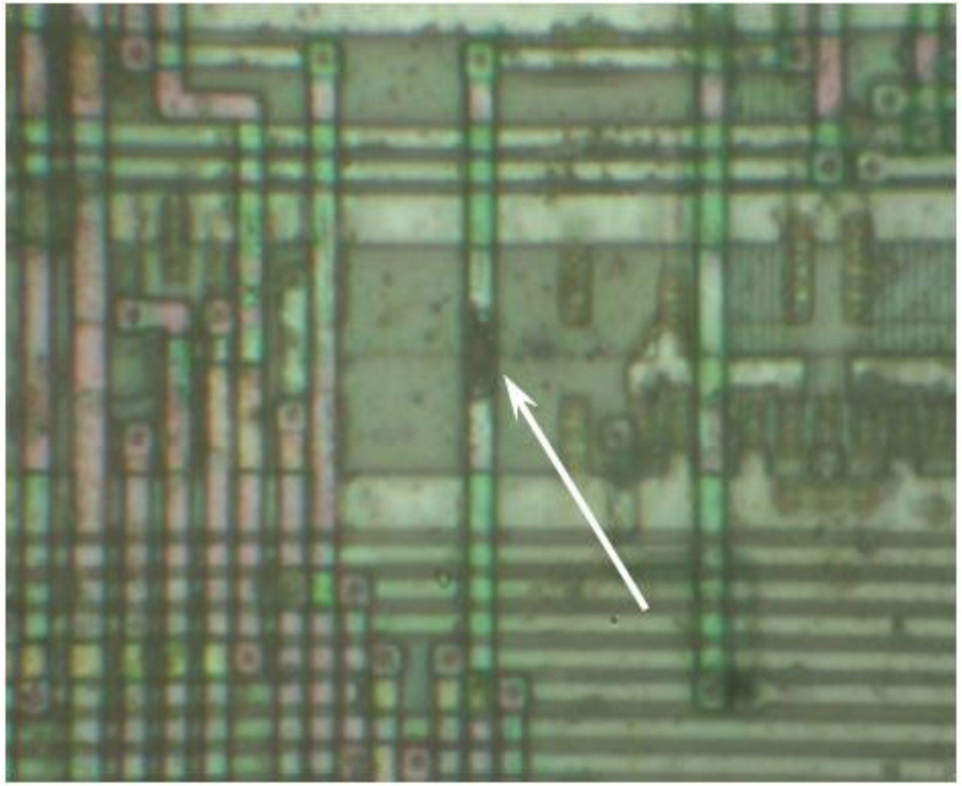


Figure 71. Cutting a single wire in the PIC12C508A microcontroller disables the security. 1000× magnification

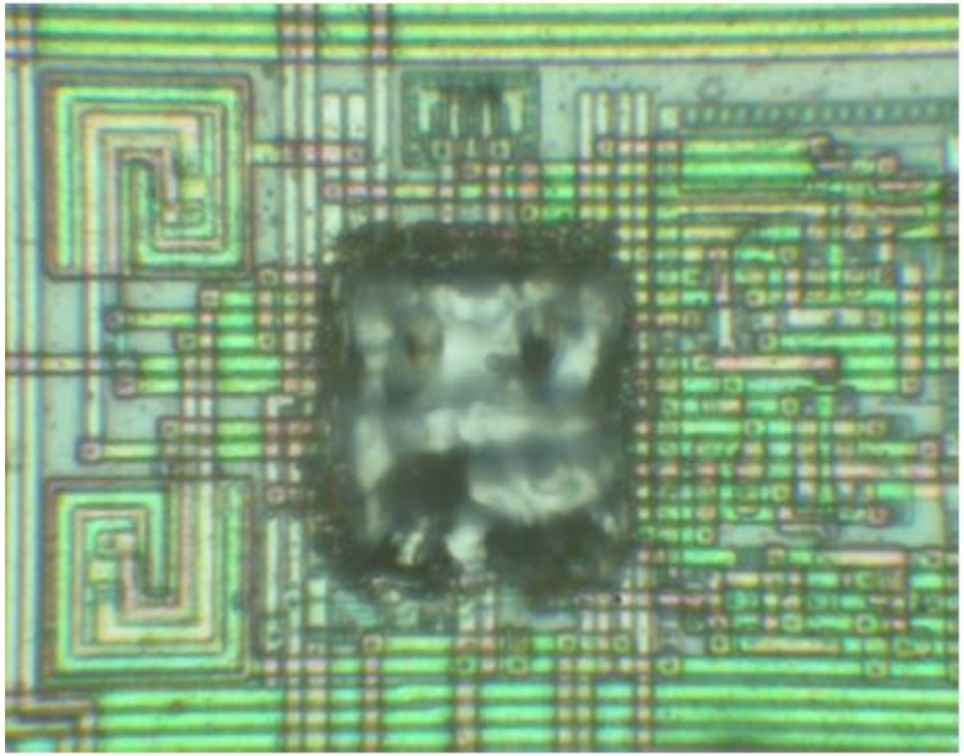


Figure 72. Disabling the security in the PIC16F628 microcontroller by destroying the fuse control circuit with a laser cutter. 500× magnification

In the left image, Security circuitry is disabled by cutting a wire.
In the right image, whole security circuitry is destroyed by laser cutting machine to disable it.