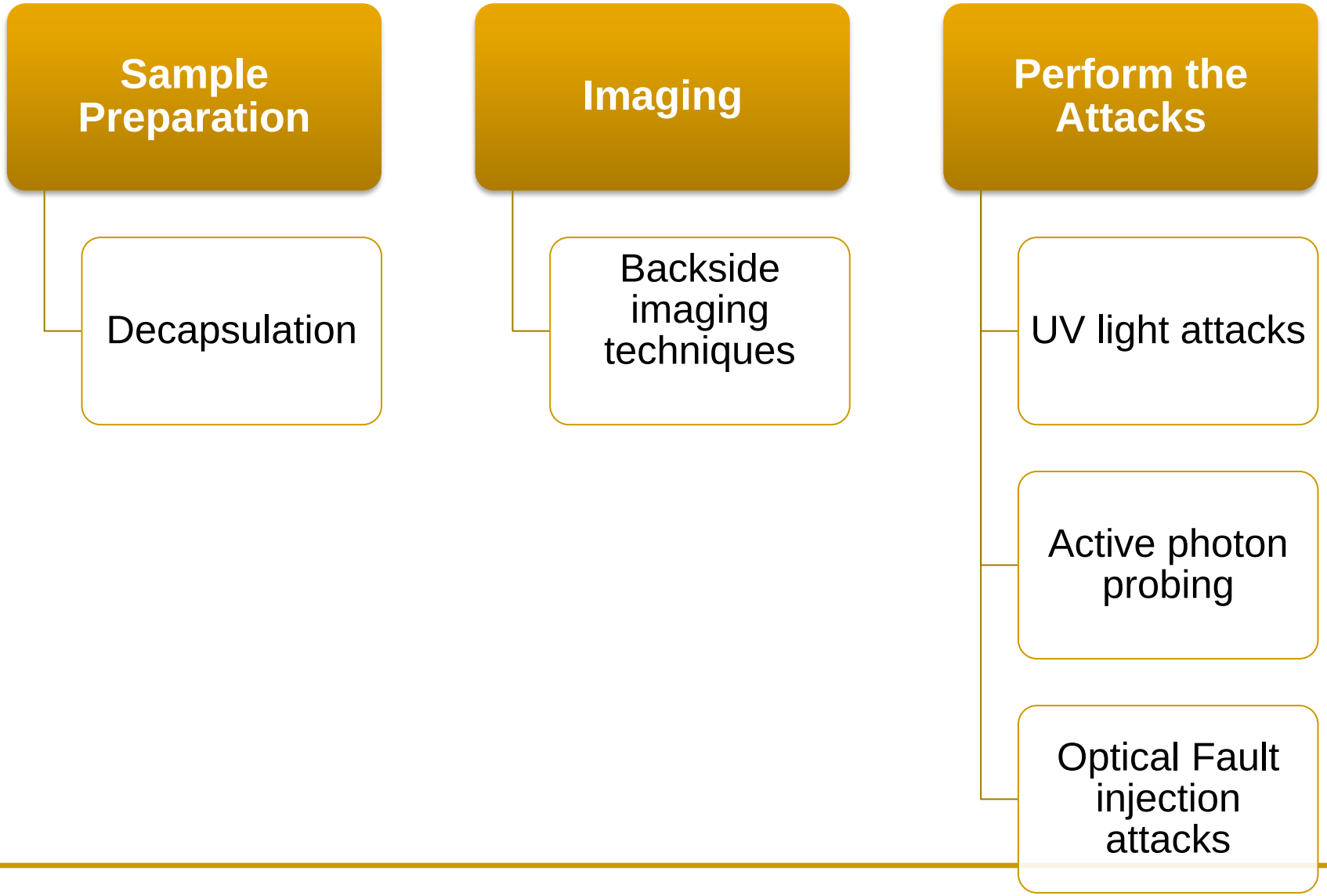
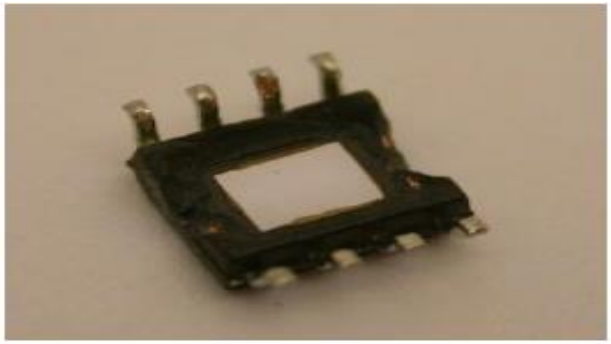
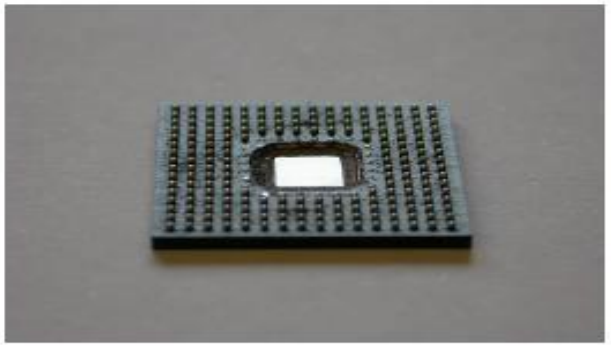
Semi-Invasive Attacks



Semi-Invasive Attacks: Sample Preparation

- Decapsulation of the chip to prepare it for attacks.
- For the modern chips, backside decapsulation is used
  - There is no need to use chemicals

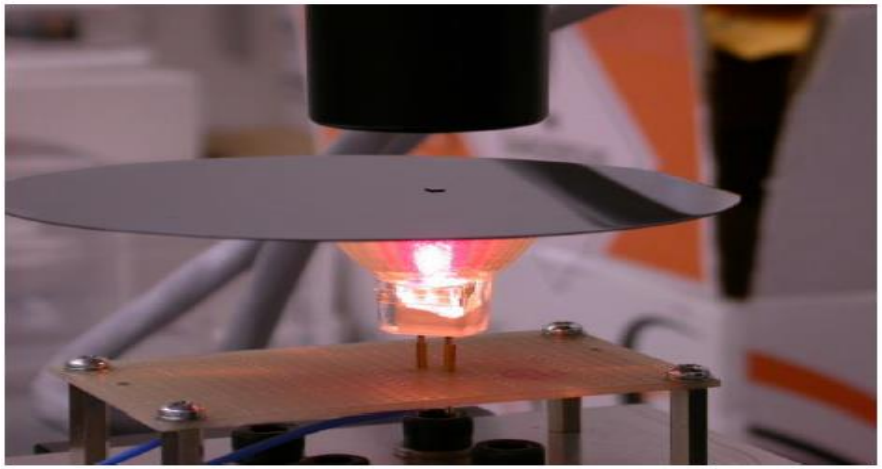




Semi-Invasive Attacks: Imaging

- 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



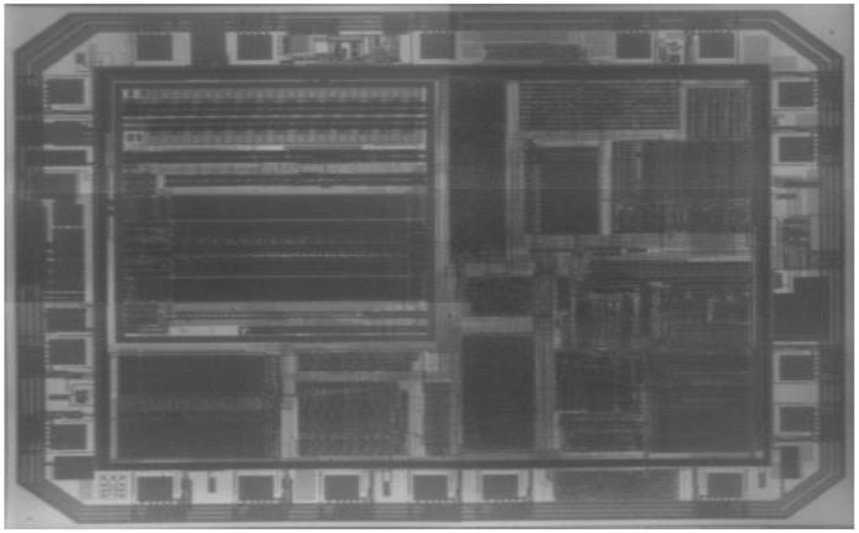
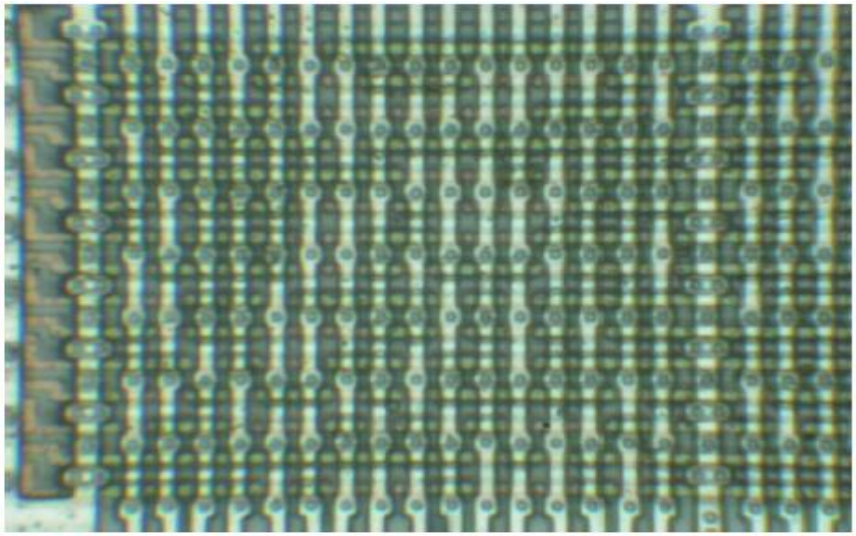


Figure 78. Transmitted light setup and image of the MSP430F112 microcontroller. 50× magnification



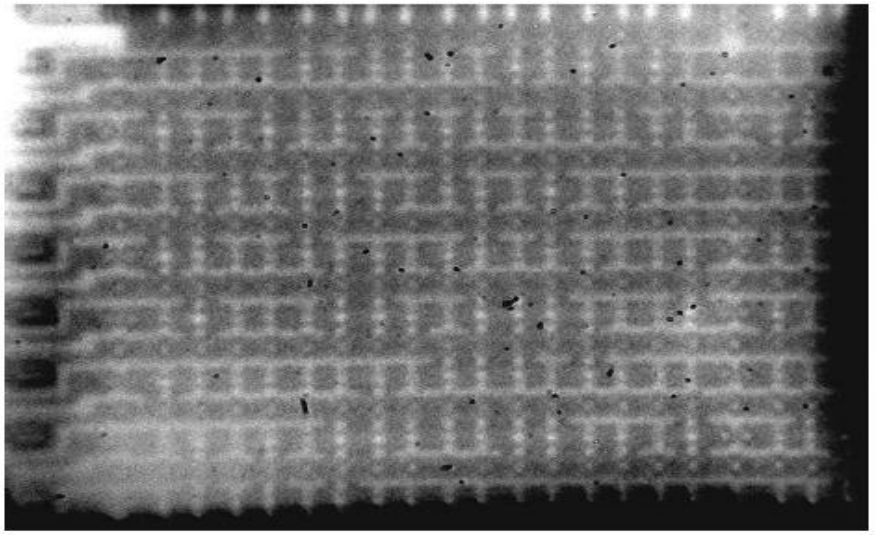
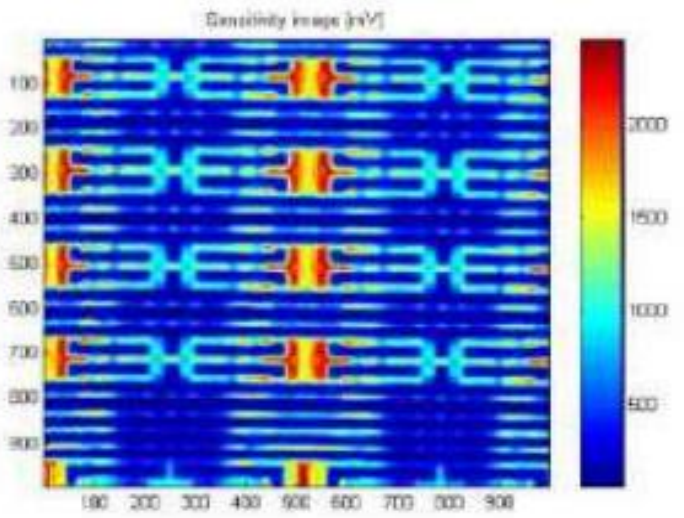


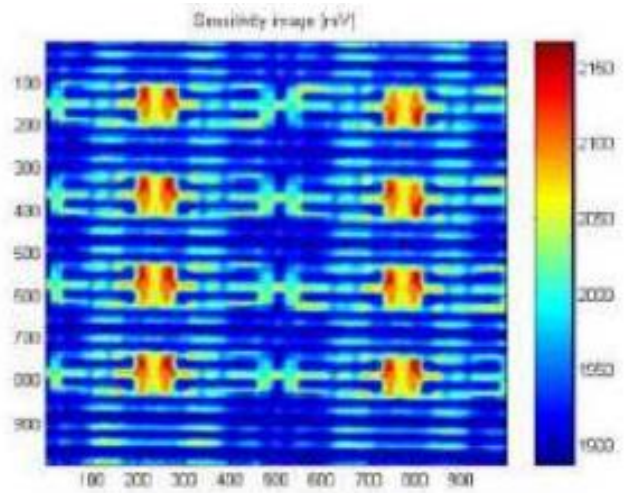
Figure 79. Standard optical image and reflected light backside image of the Mask ROM inside MC68HC705P6A microcontroller built with 1.0 µm technology. 500× magnification

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

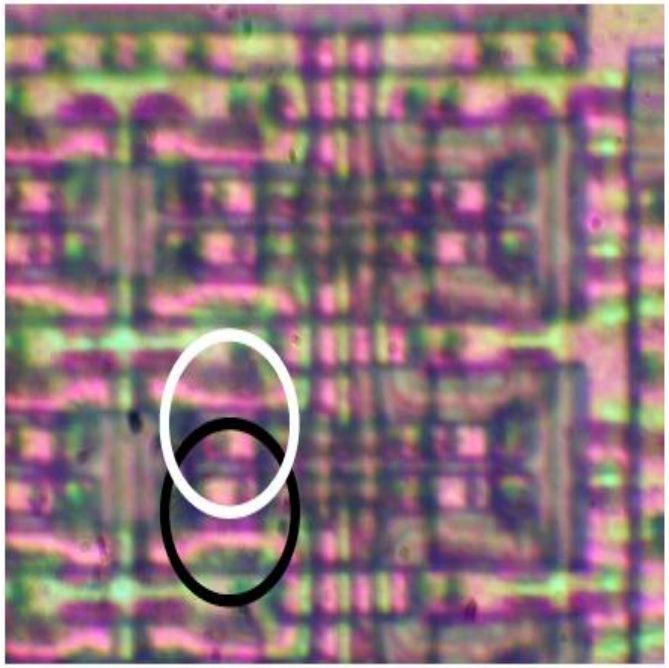


Figure 91. SRAM memory array with maximum magnification (1500×)

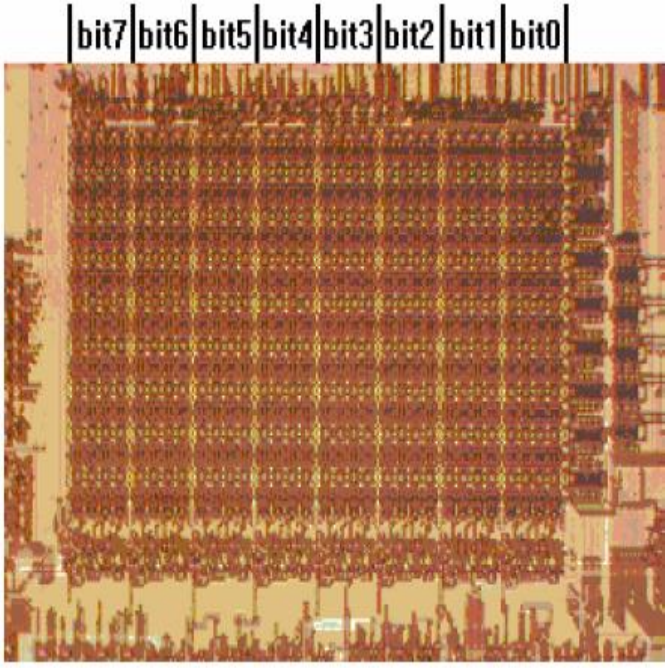


Figure 92. Allocation of data bits in SRAM memory array

- Focusing the light spot from the lamp on the area shown by the white circle caused the cell to change its state from '1' to '0', with no change if the state was already '0'.
- By focusing the spot on the area shown by the black circle, the cell changed its state from '0' to '1' or remained in state '1'.

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