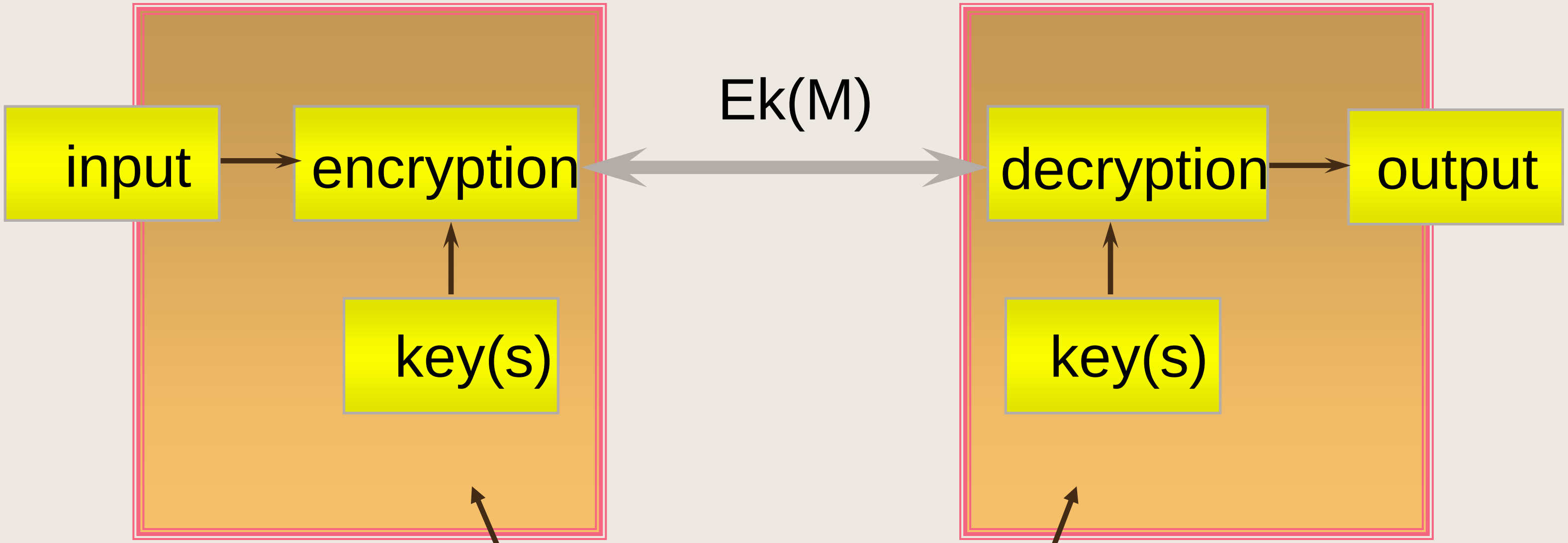
brightsight®

your
partner
in security
approval

Physical Attacks on Cryptographic devices

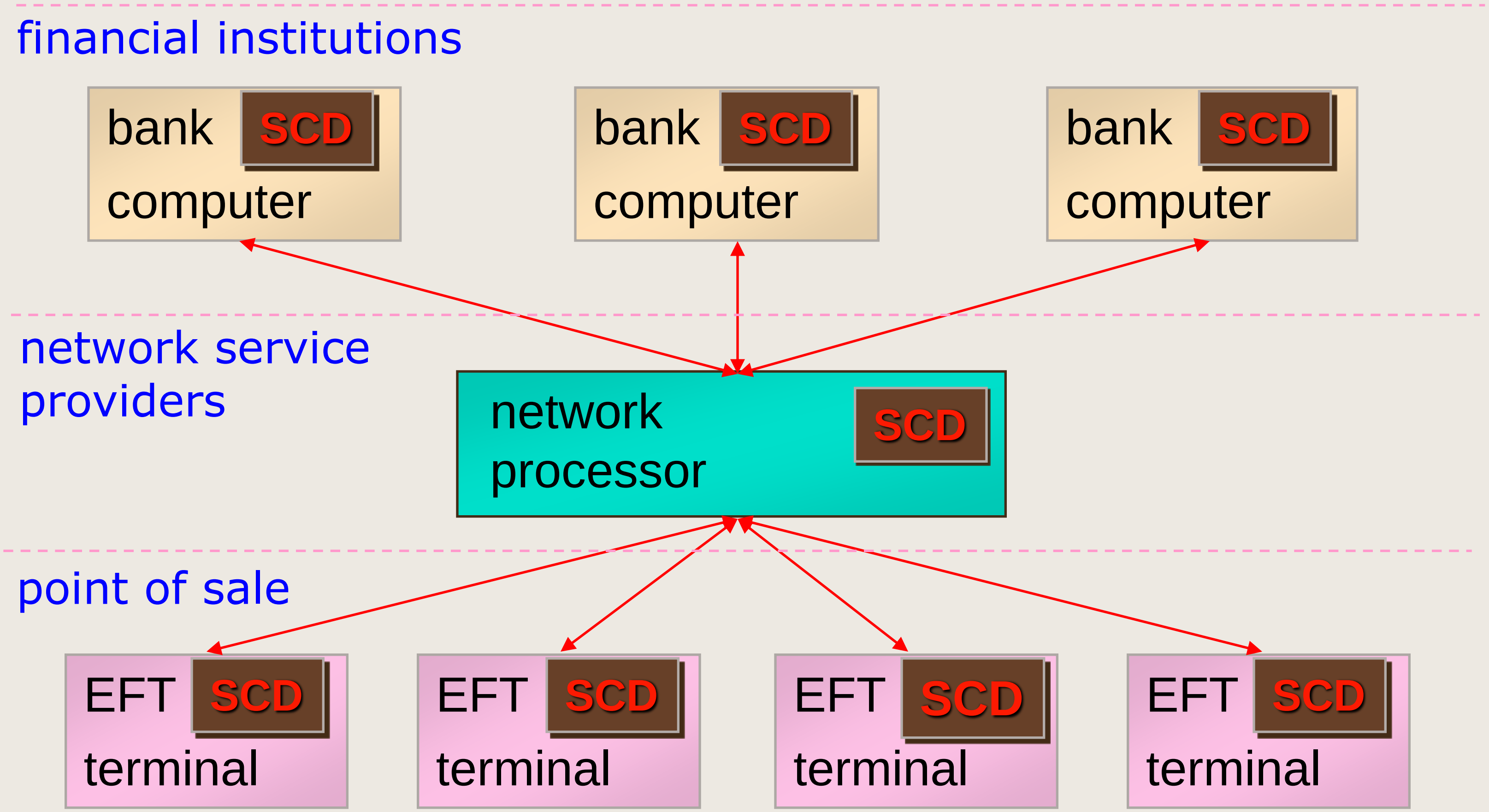
How to break into today's cryptographic hardware

Cryptography applied in IT systems



Secure Cryptographic
Devices (SCD's)

General secure banking system



financial institutions

bank computer SCD

bank computer SCD

bank computer SCD

network service providers

network processor SCD

point of sale

EFT terminal SCD

EFT terminal SCD

EFT terminal SCD

EFT terminal SCD

Some general security viewpoints:

- 100% Security is never possible (everything can be broken)
- All design information is known or can be retrieved
- Breaking of one device may not lead to breaking of the entire system
- Weak aspects should be covered by other security measures
- Security has to be provided by the complete system

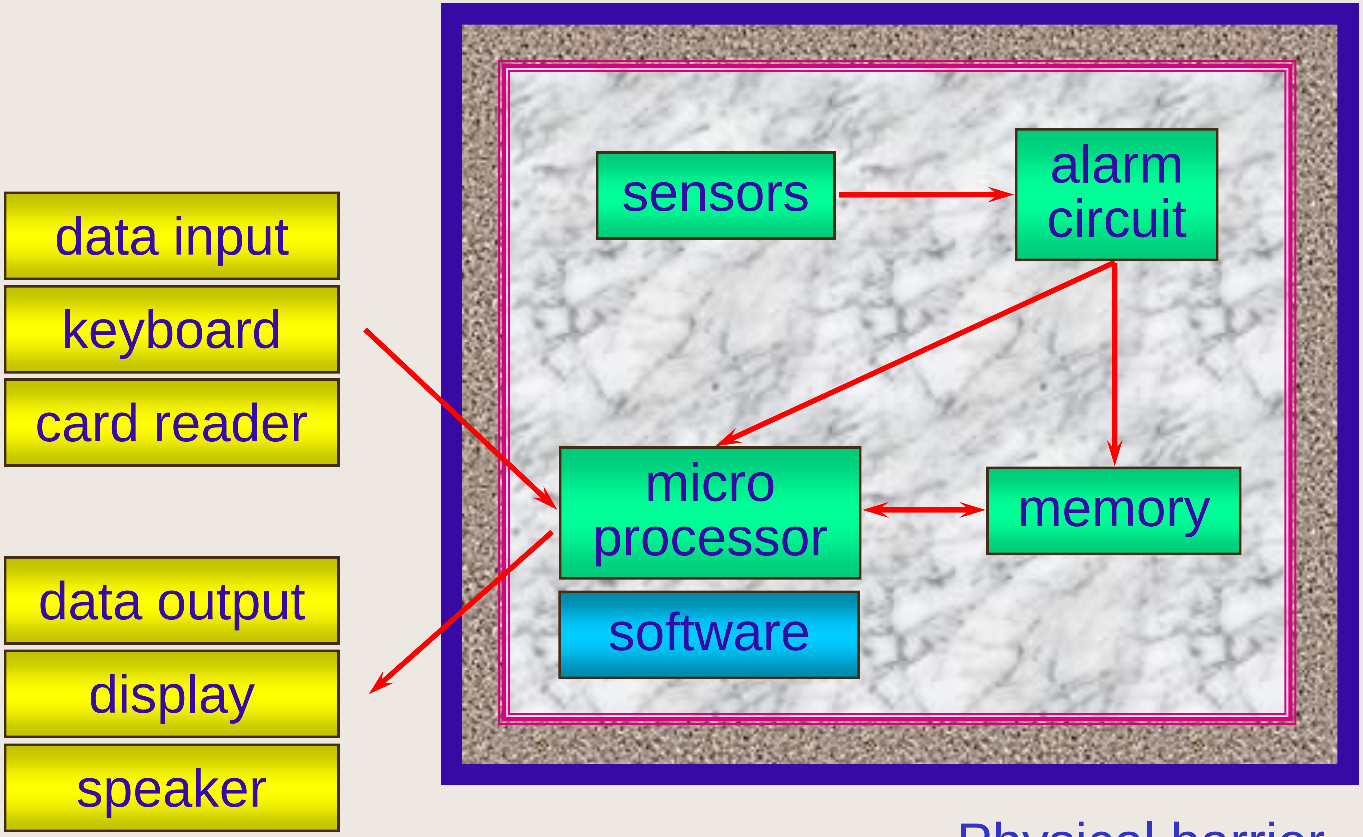
Secure Cryptographic Device

Security functions:

- Storage of sensitive data:
  - Cryptographic keys
  - PIN codes
  - User data

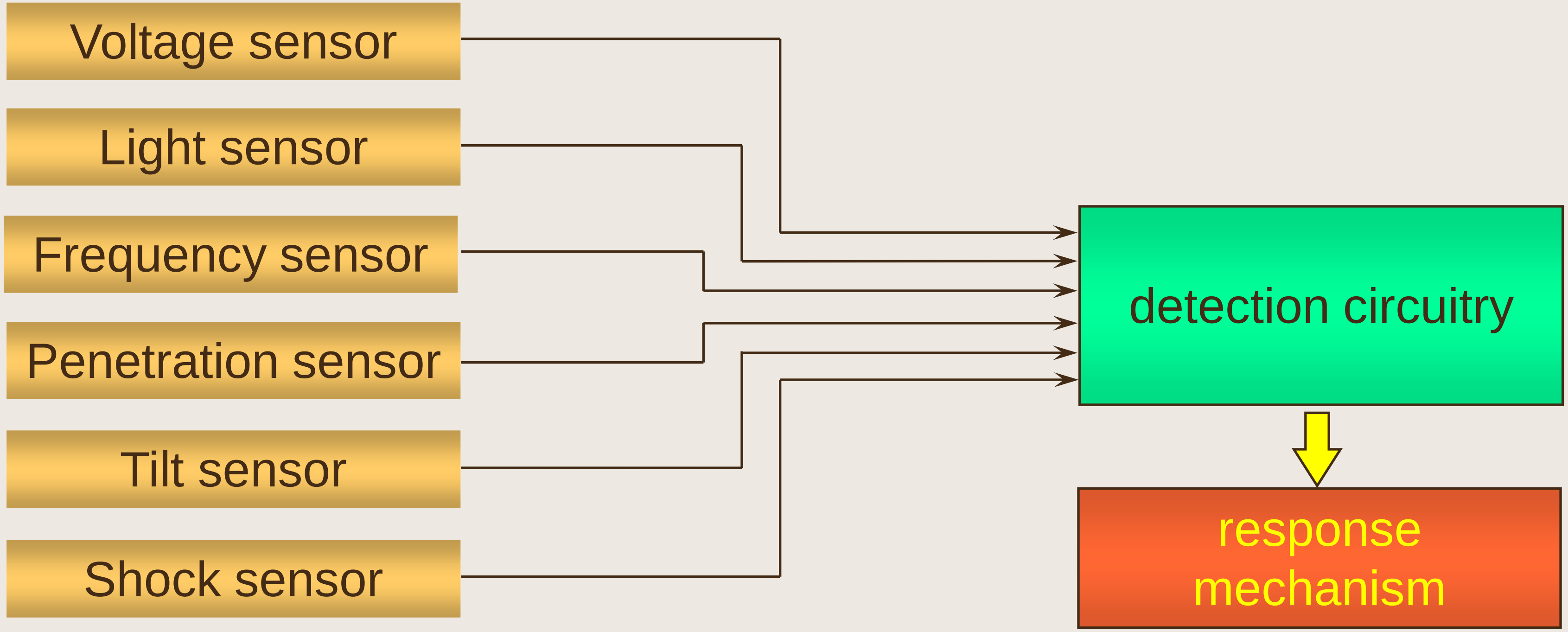
- Examples:
  - PIN Entry Devices (PED’s)
  - Host Security Modules (HSM’s)
  - Smart Cards
  - Secure USB sticks
  - Set-top boxes
  - Trusted Platform Modules (TPM’s) in phones, computers…
  - FPGA configuration storage

Secure Cryptographic Device

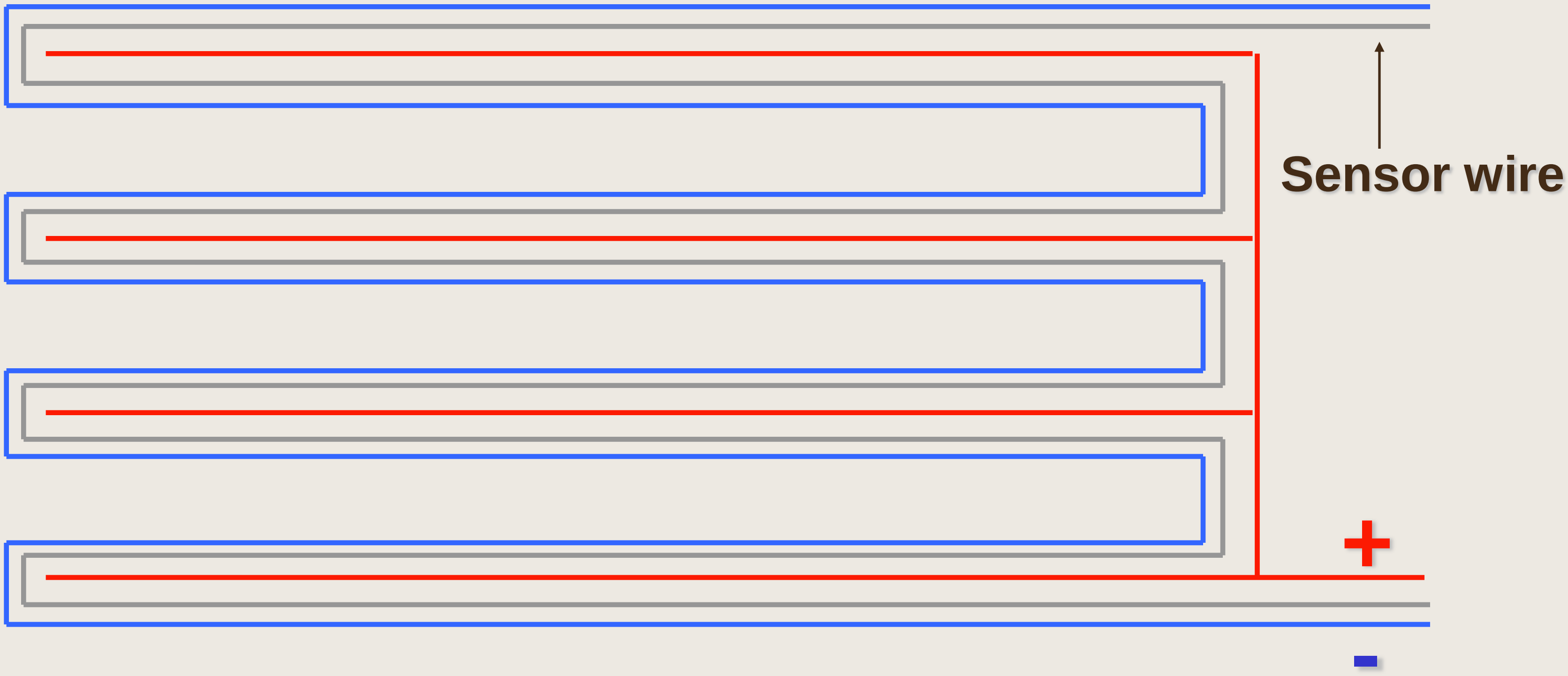


Physical barrier

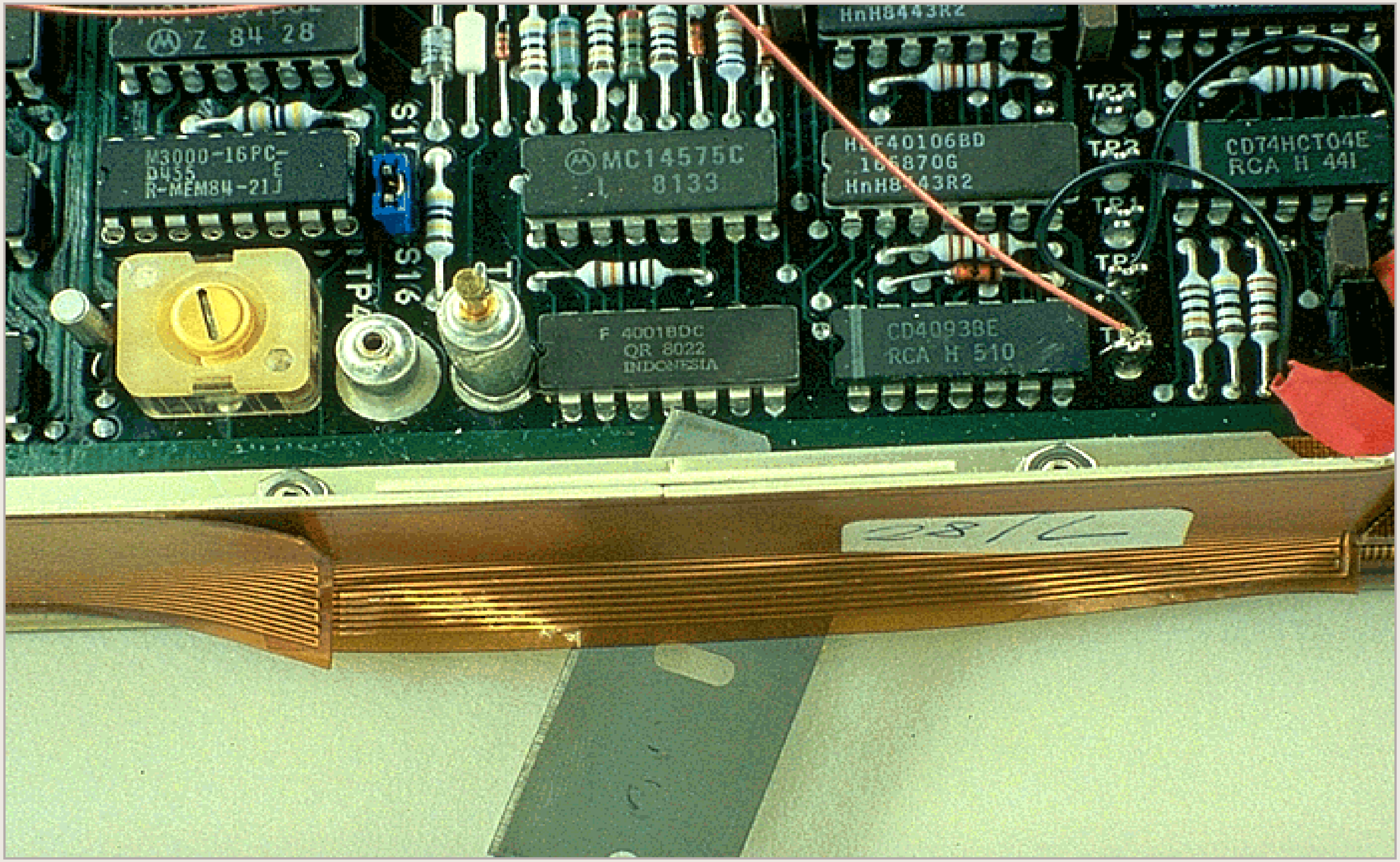
Fraud detection



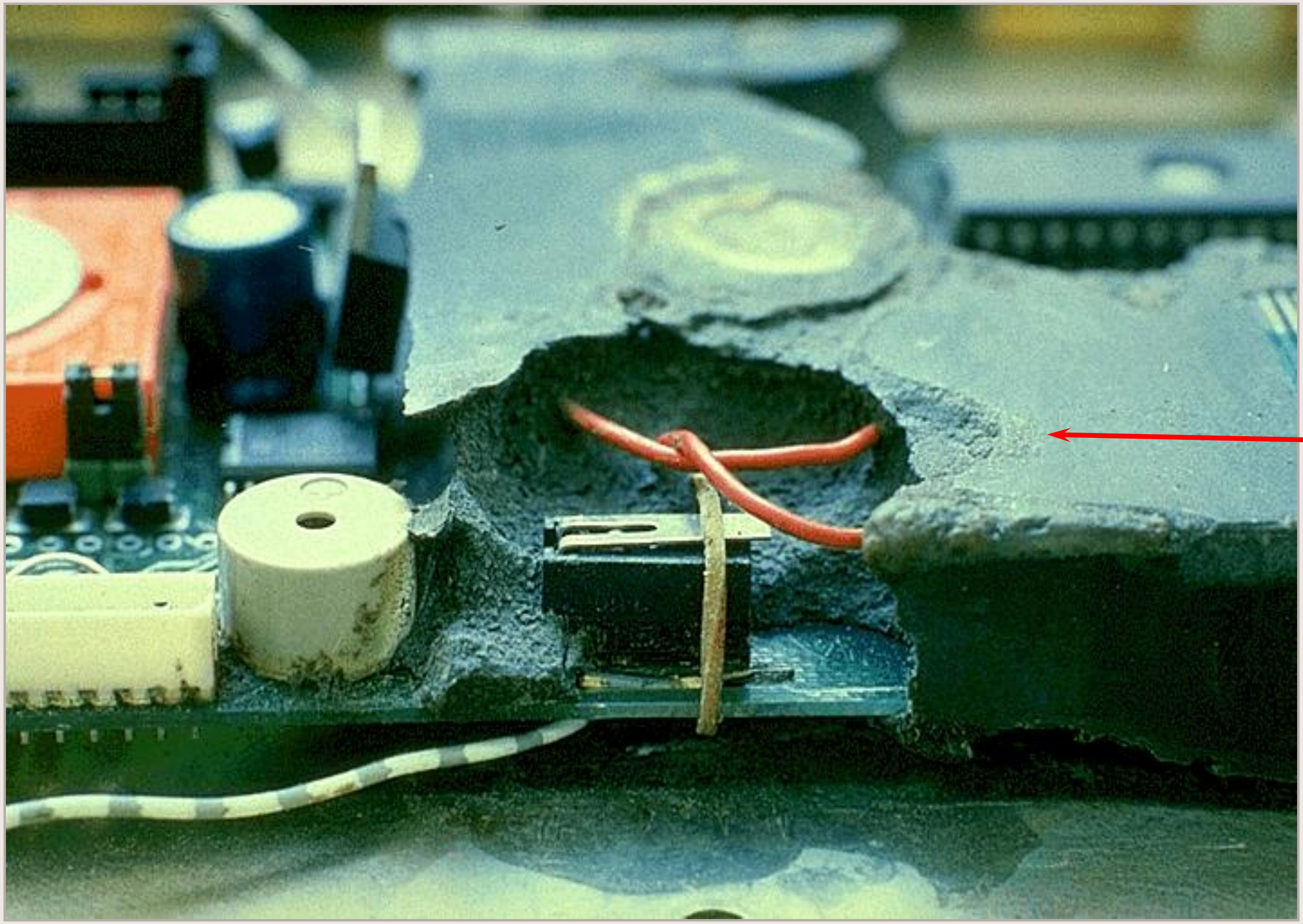
Penetration sensor



Penetration sensor

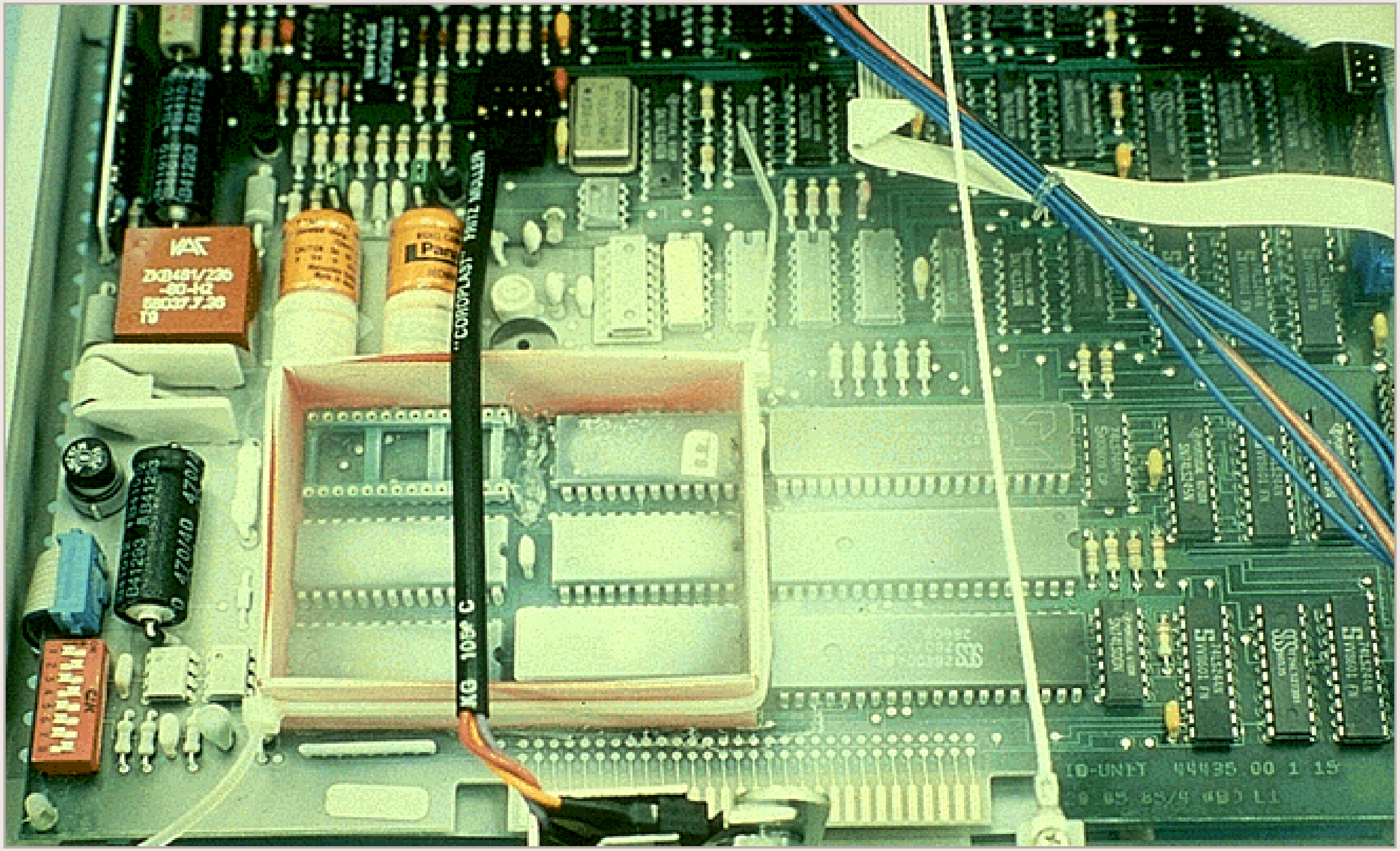


Epoxy resin

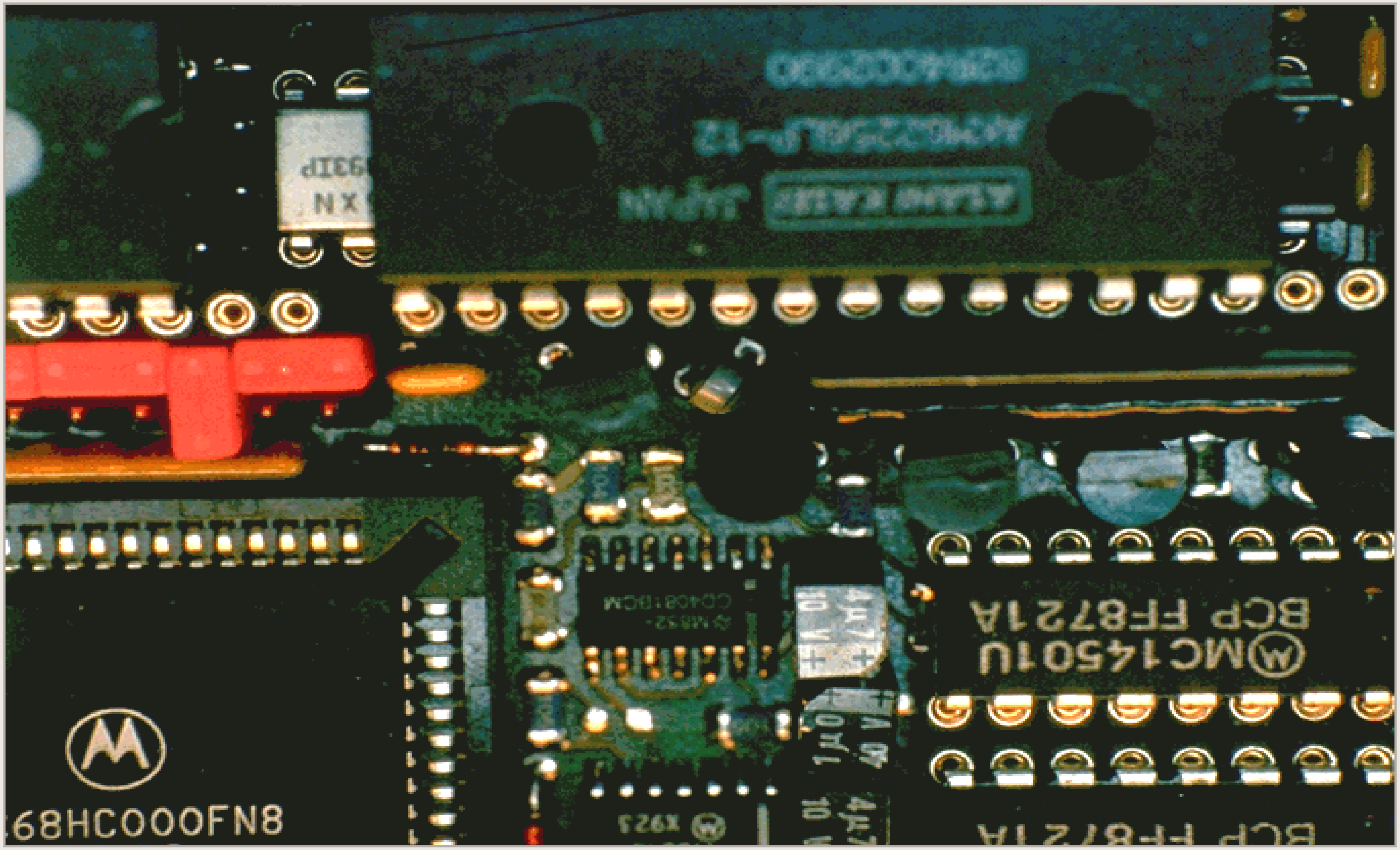


epoxy resin

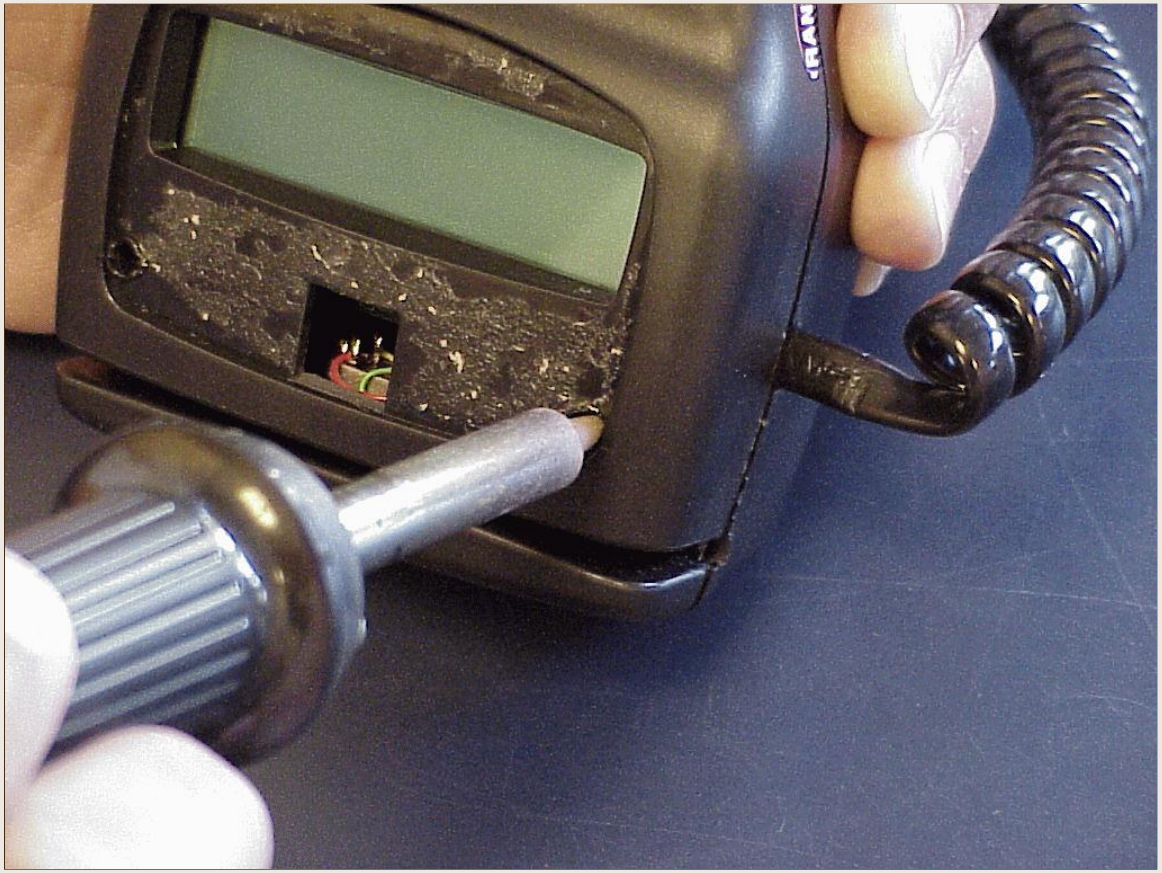
Freezing attack



Temperature sensor

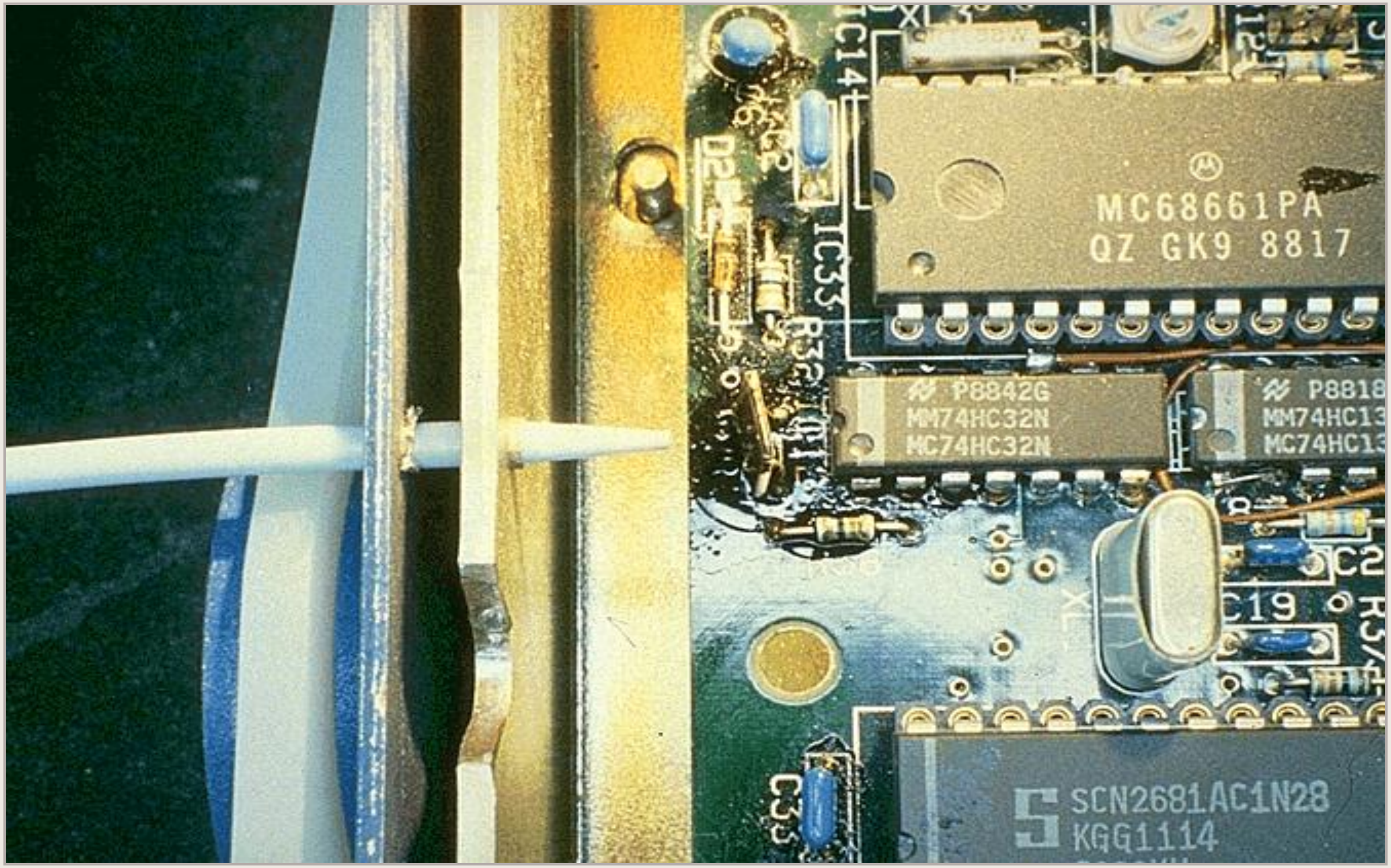


Apply heat at appropriate locations

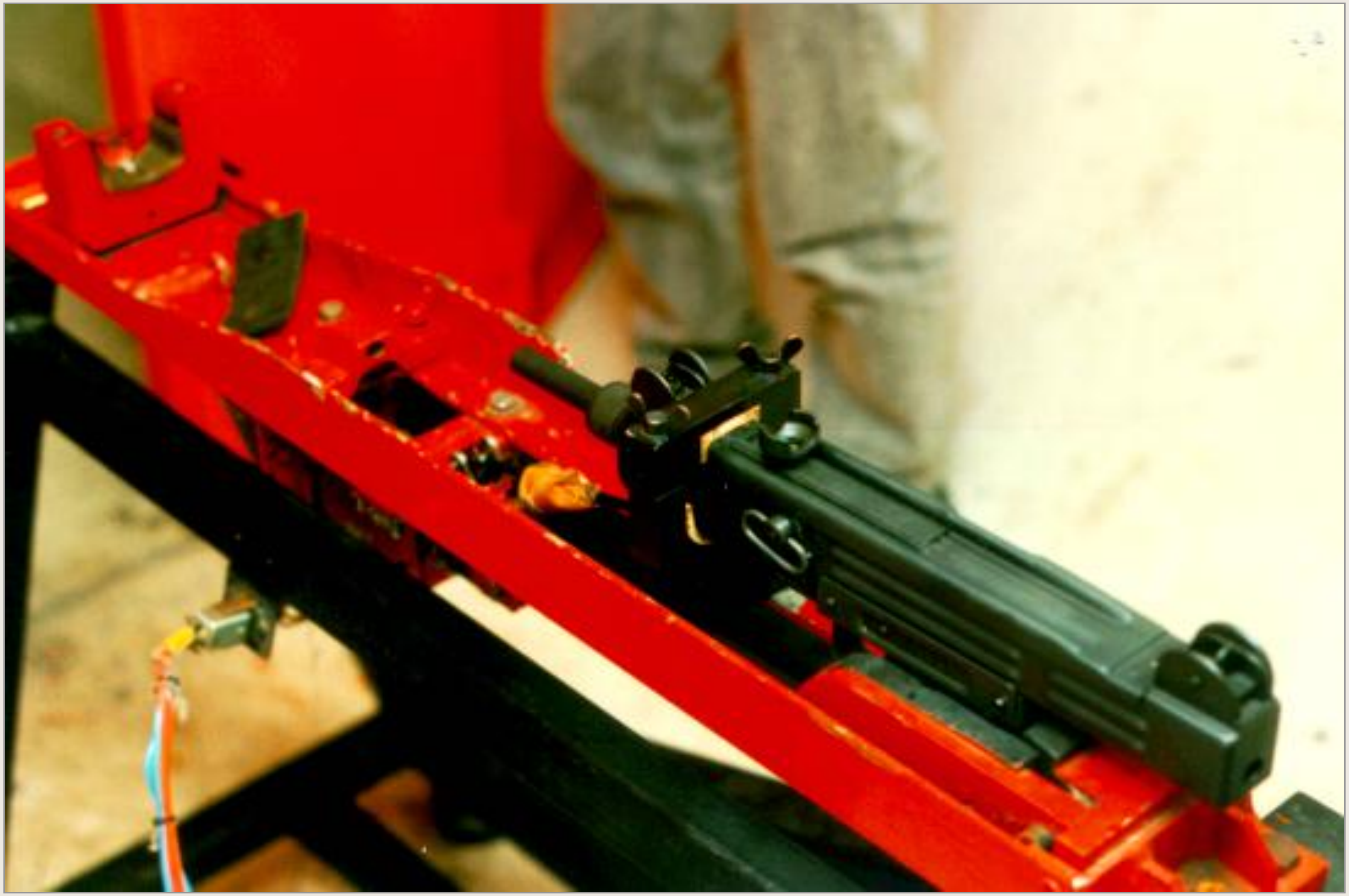


Removal of one-way screws via the front

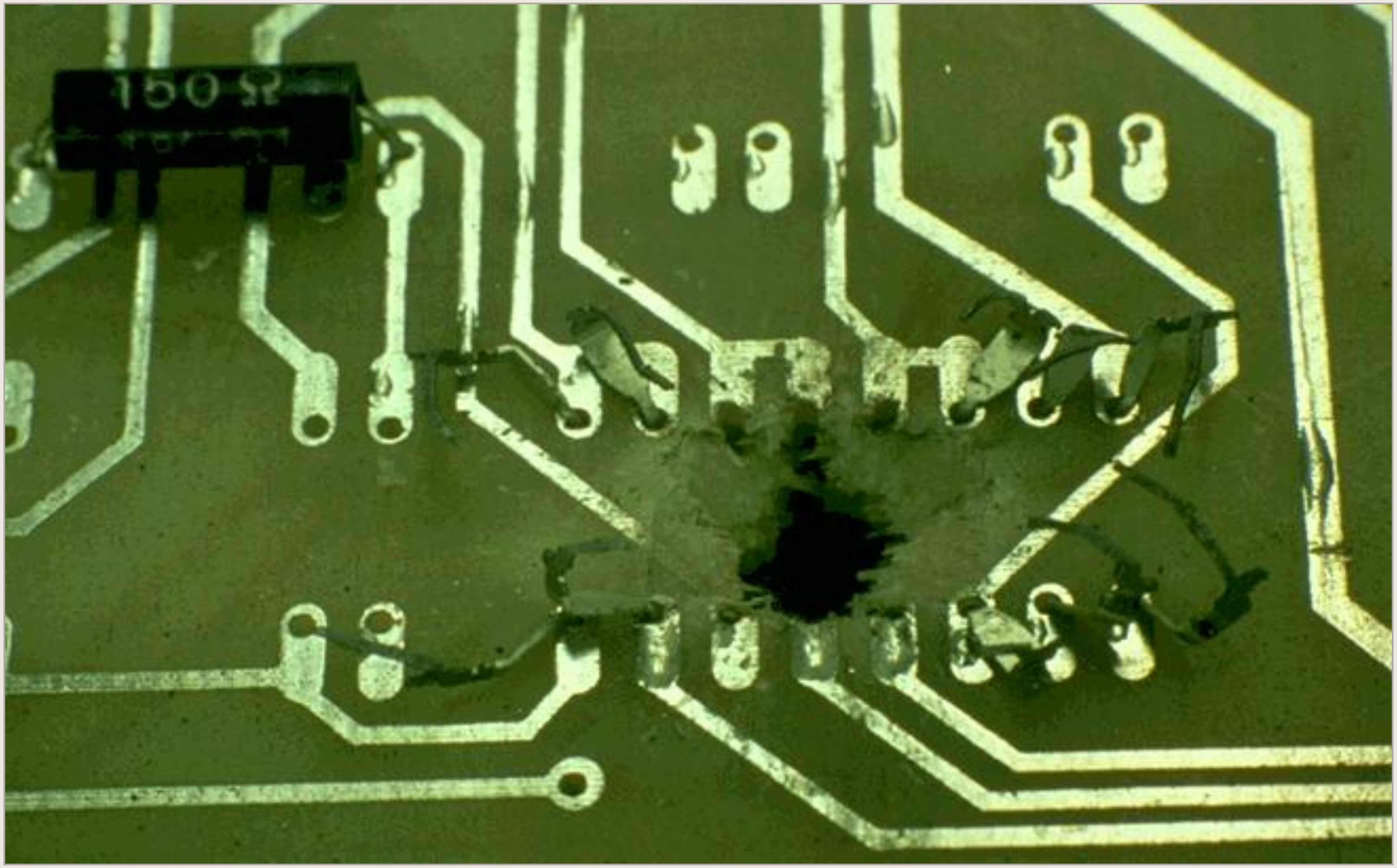
Light sensor



Evaluation methods

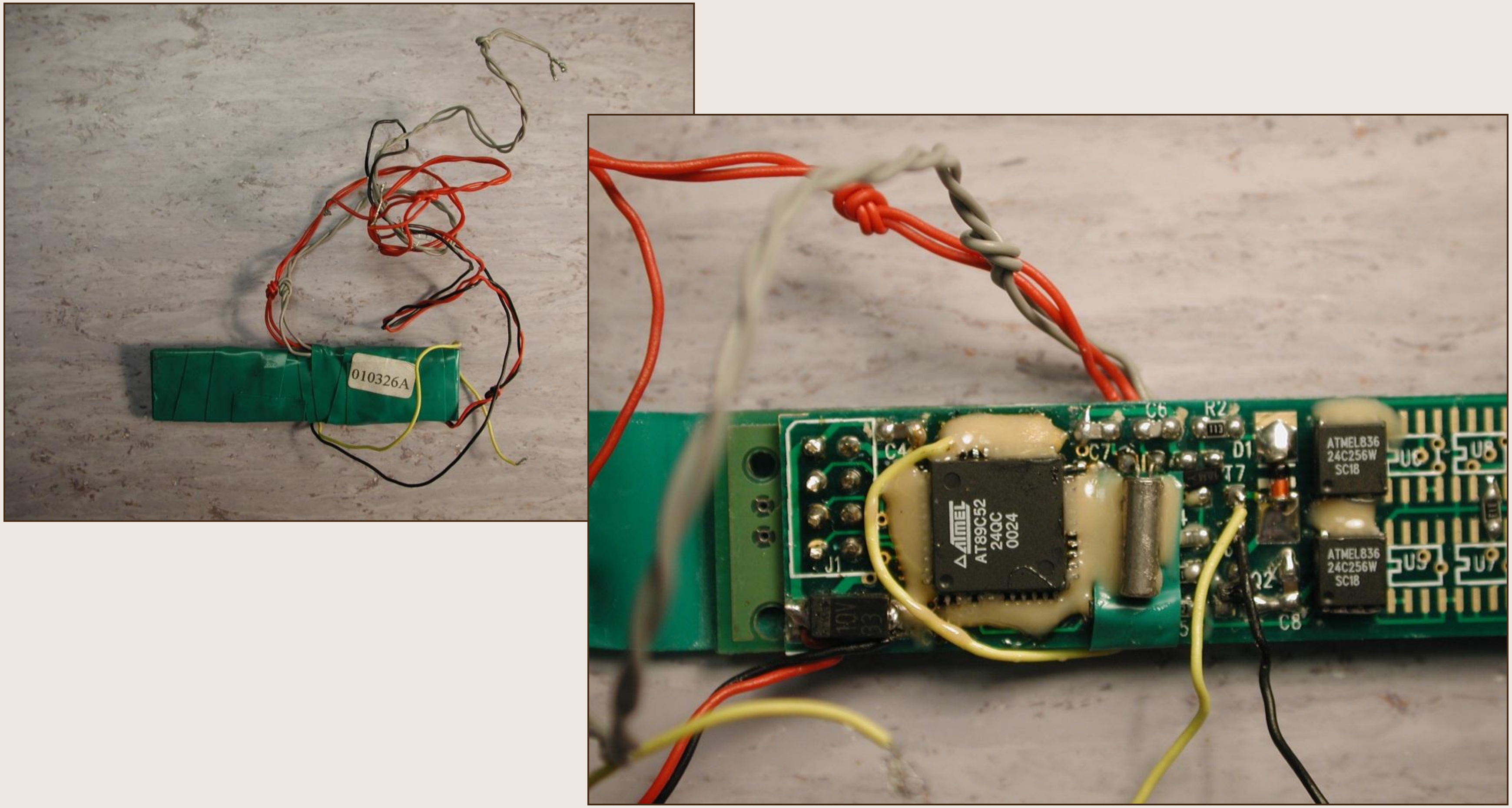


Evaluation methods

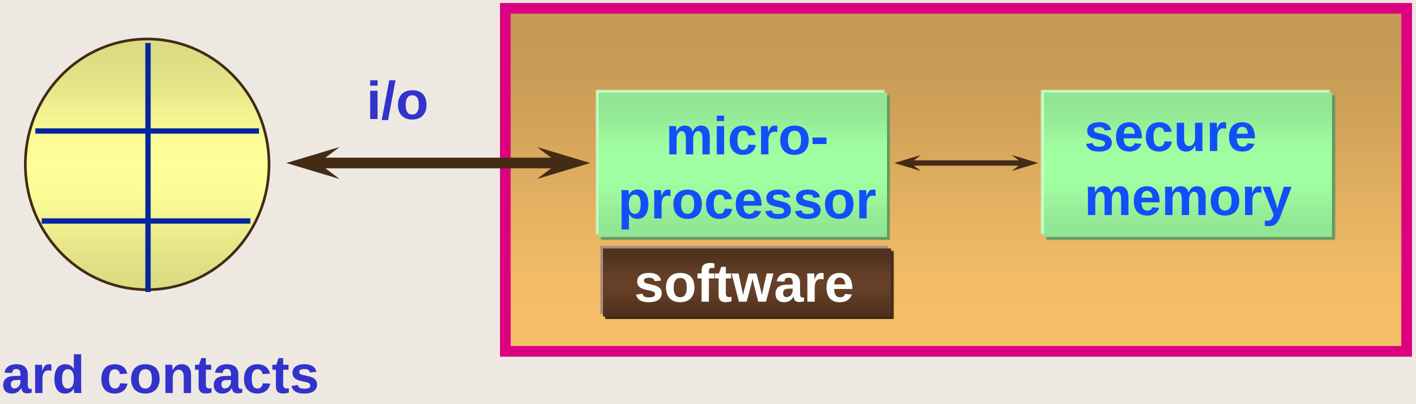


Real-life bug examples

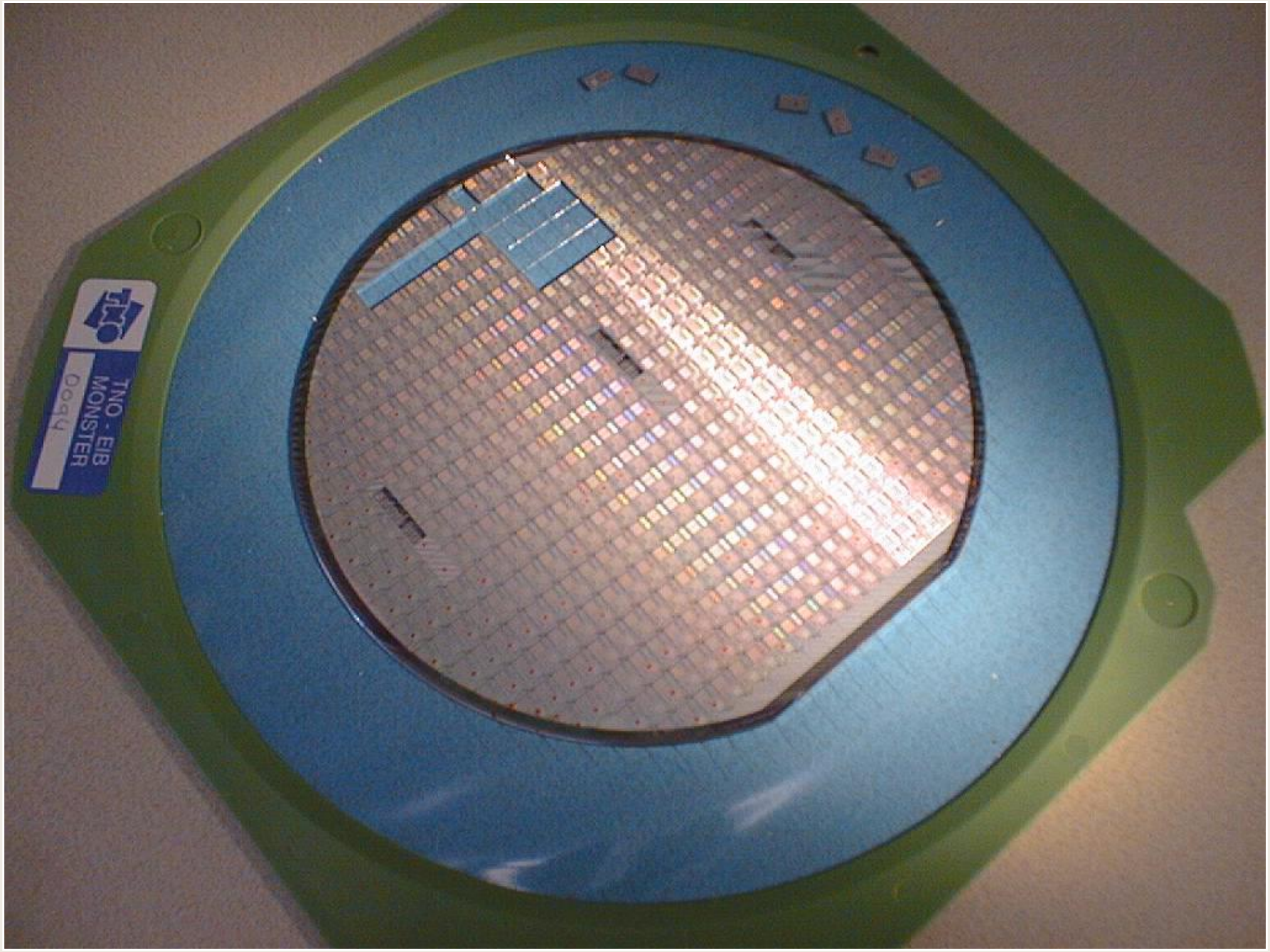
- Hardware bug fits in a PED for tapping magnetic stripe data



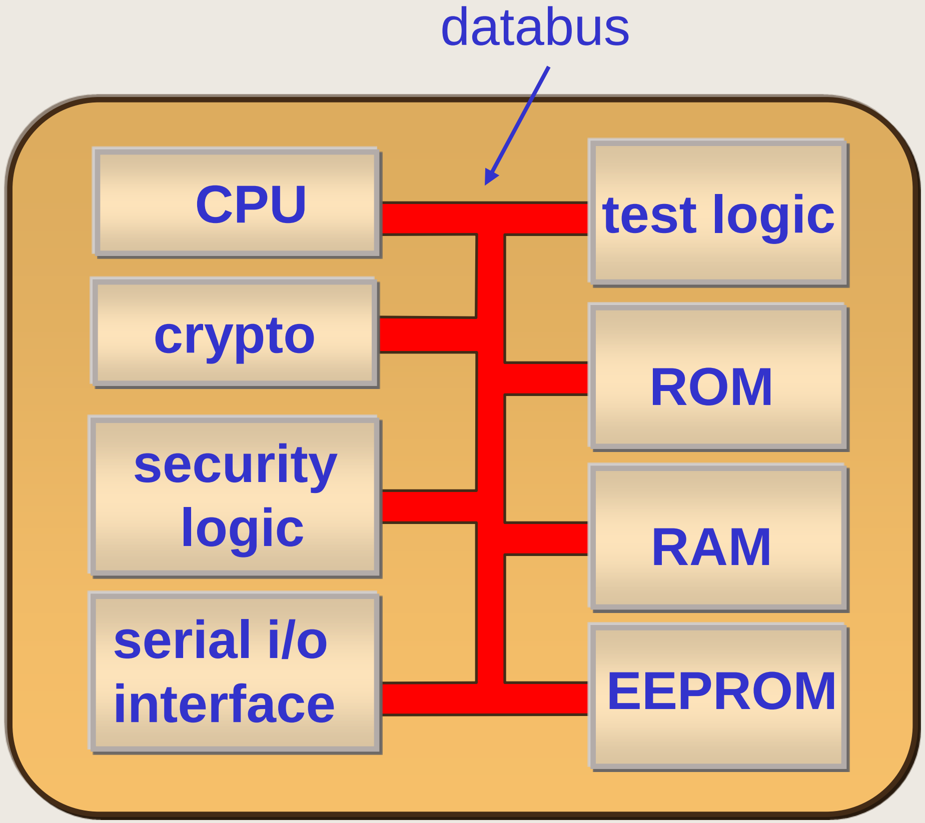
Smart card



Silicon wafer

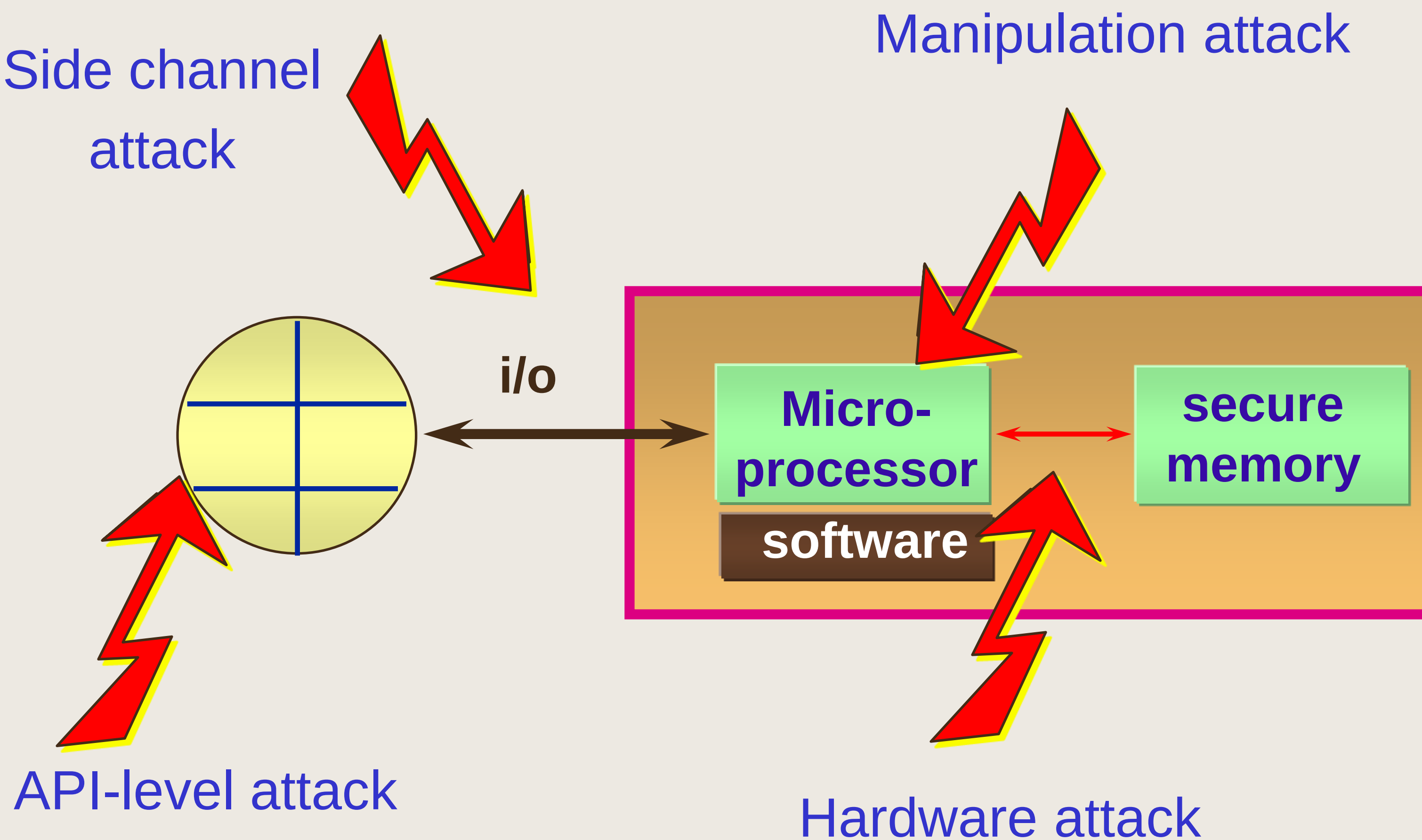


What’s inside a smart card ?

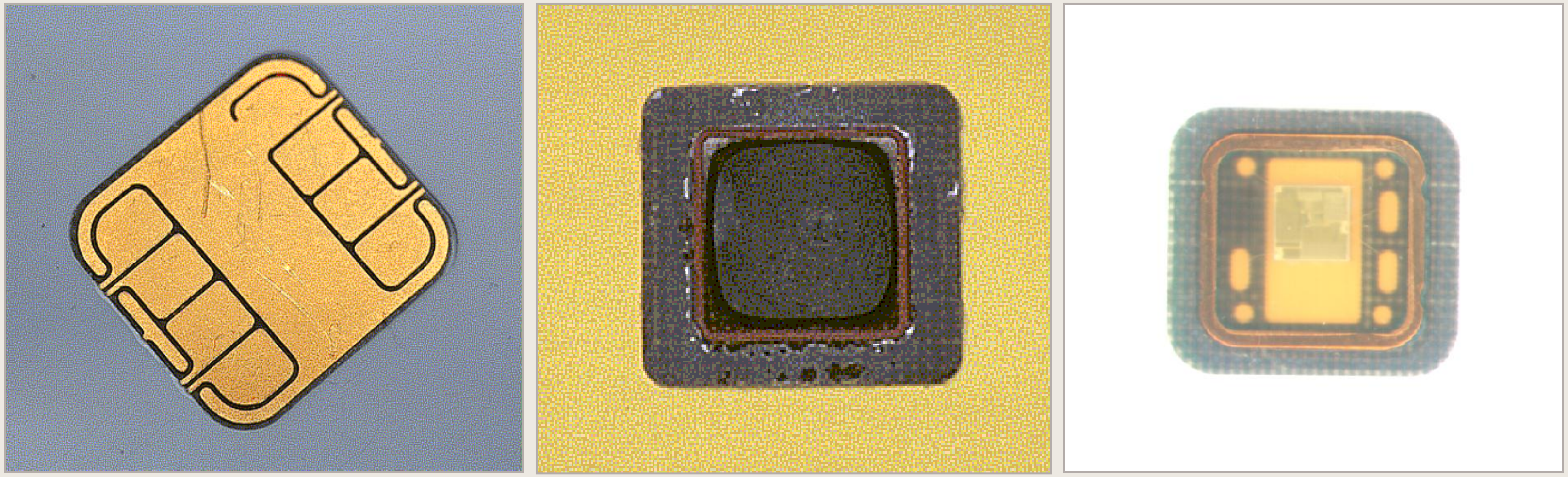


databus:
connection between building blocks

General smart card attack methods



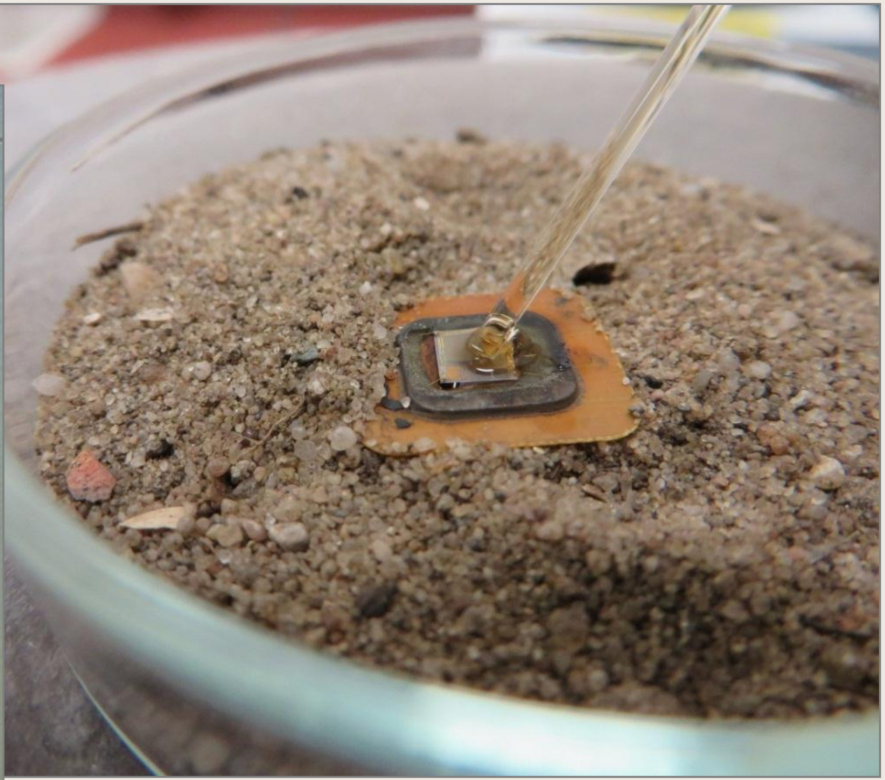
Hardware attacks on smart cards



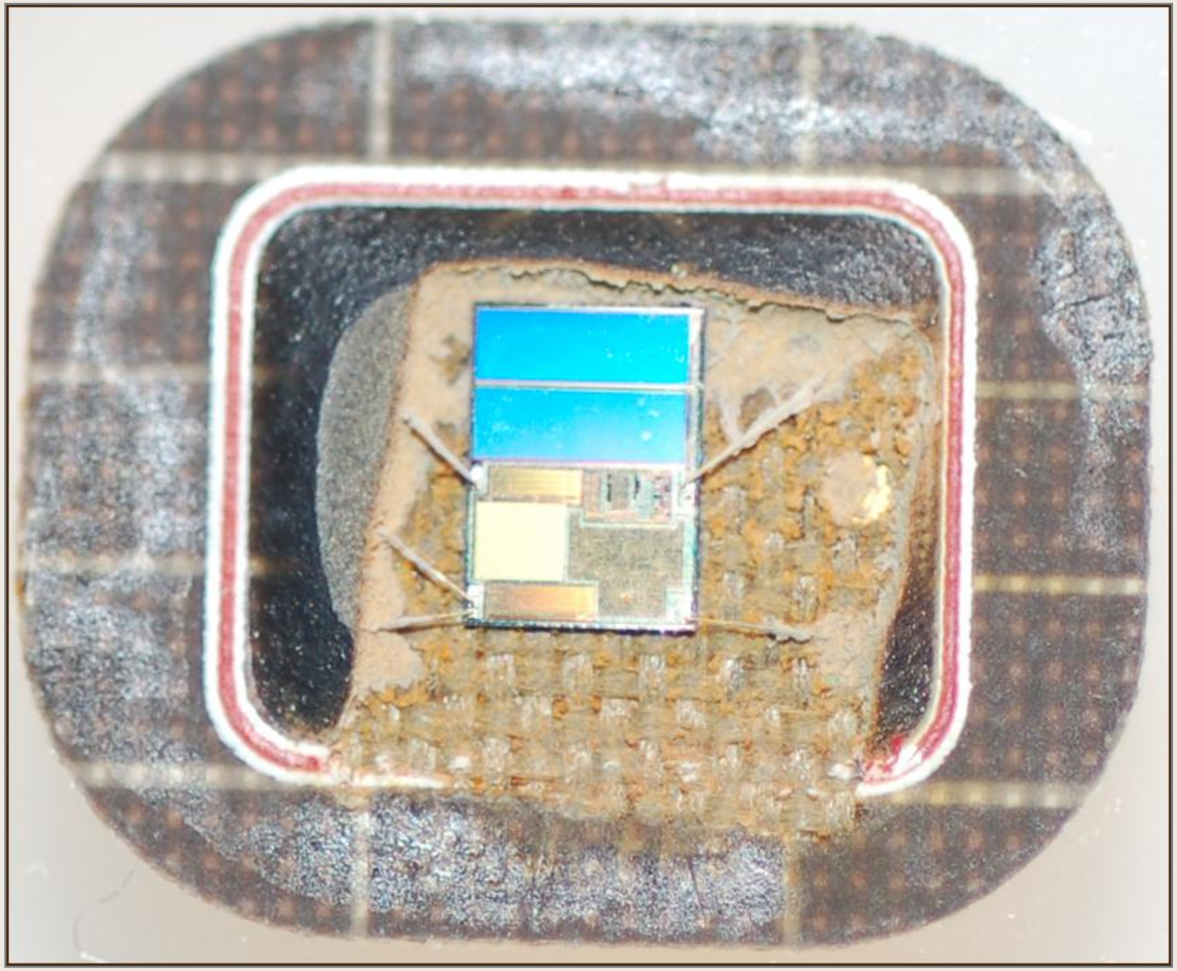
Etching with fuming Nitric acid

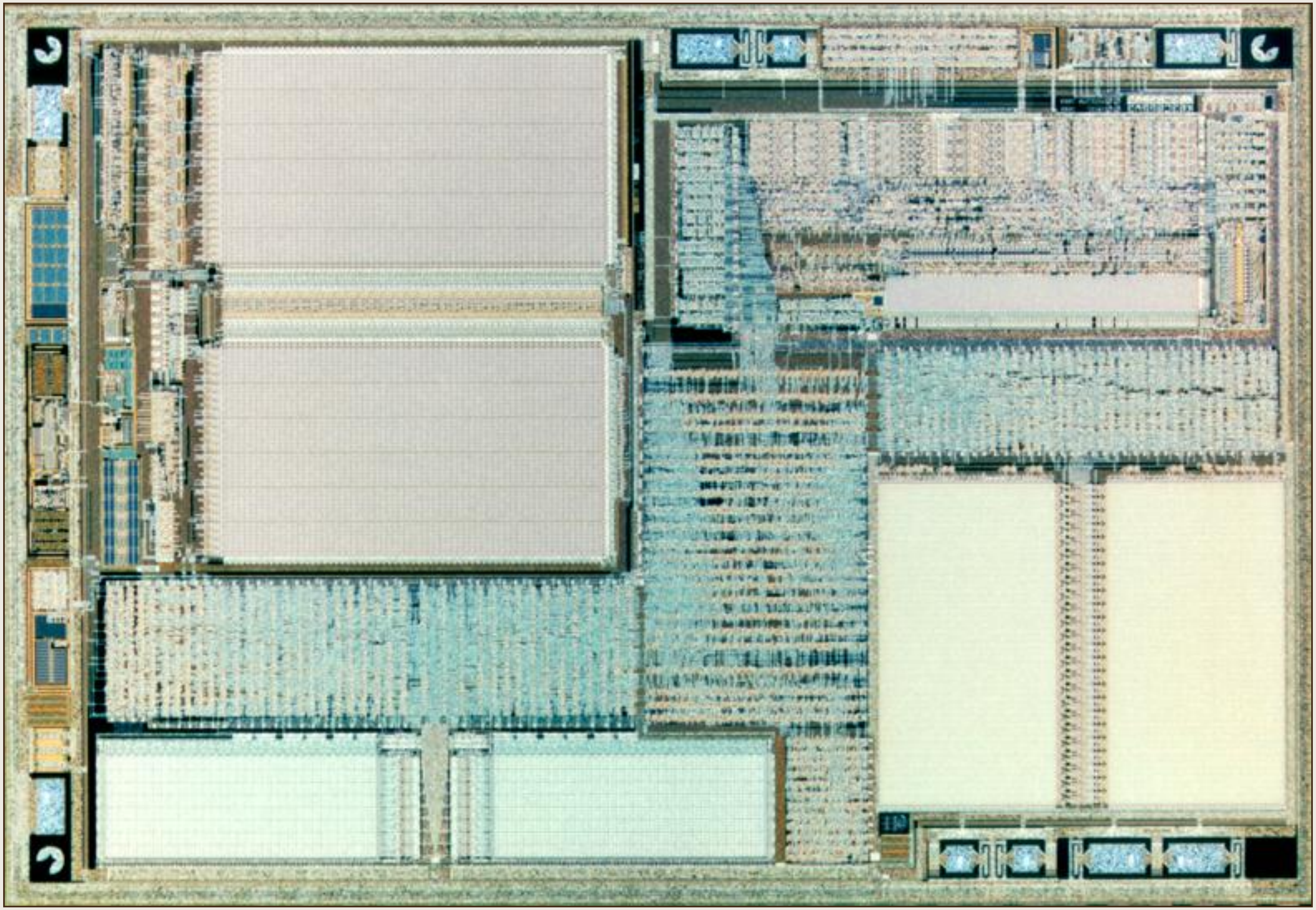
Opening of chip enclosure

- ‘Poor-mans’ way

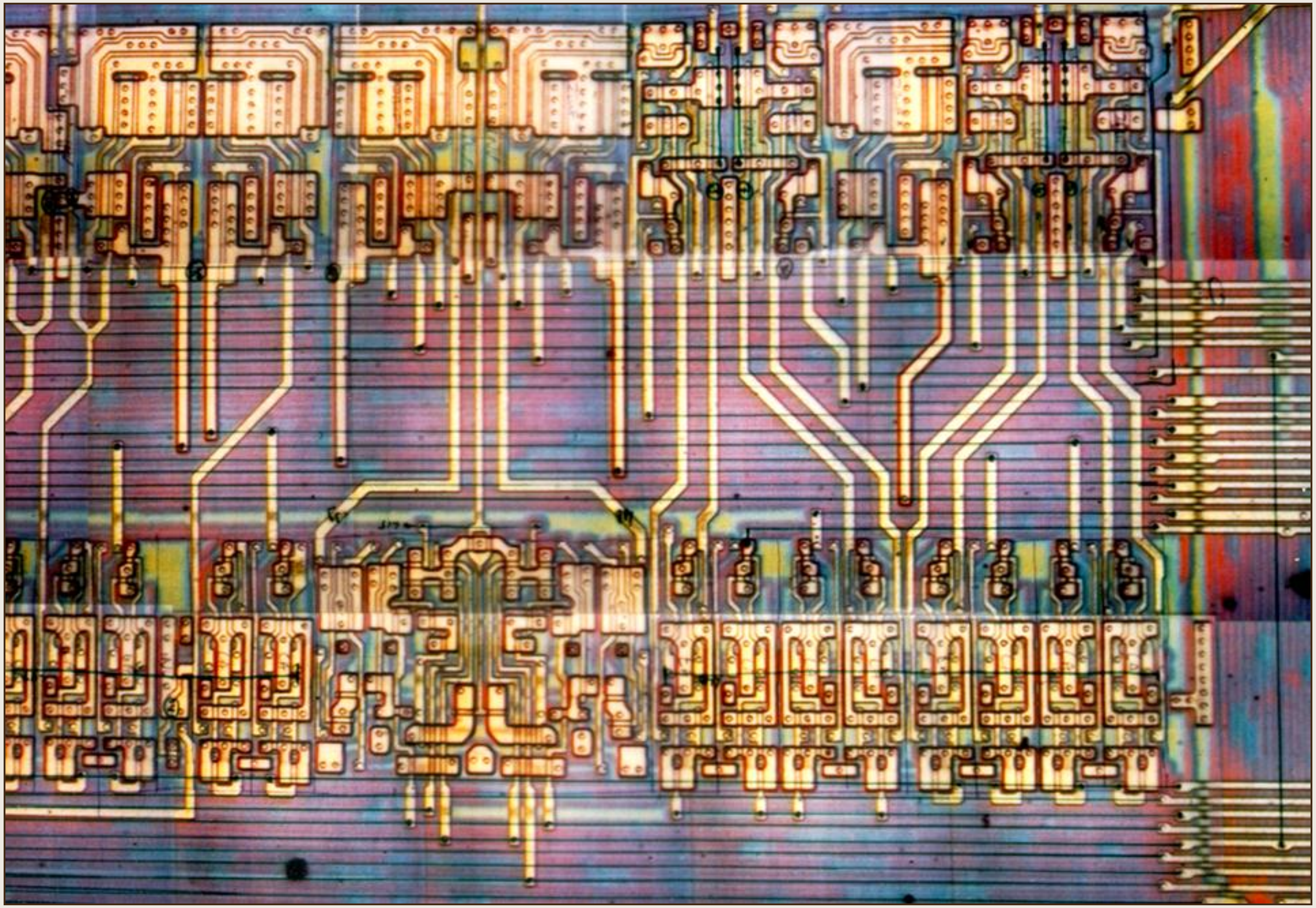


Result of etching process





Reverse engineering

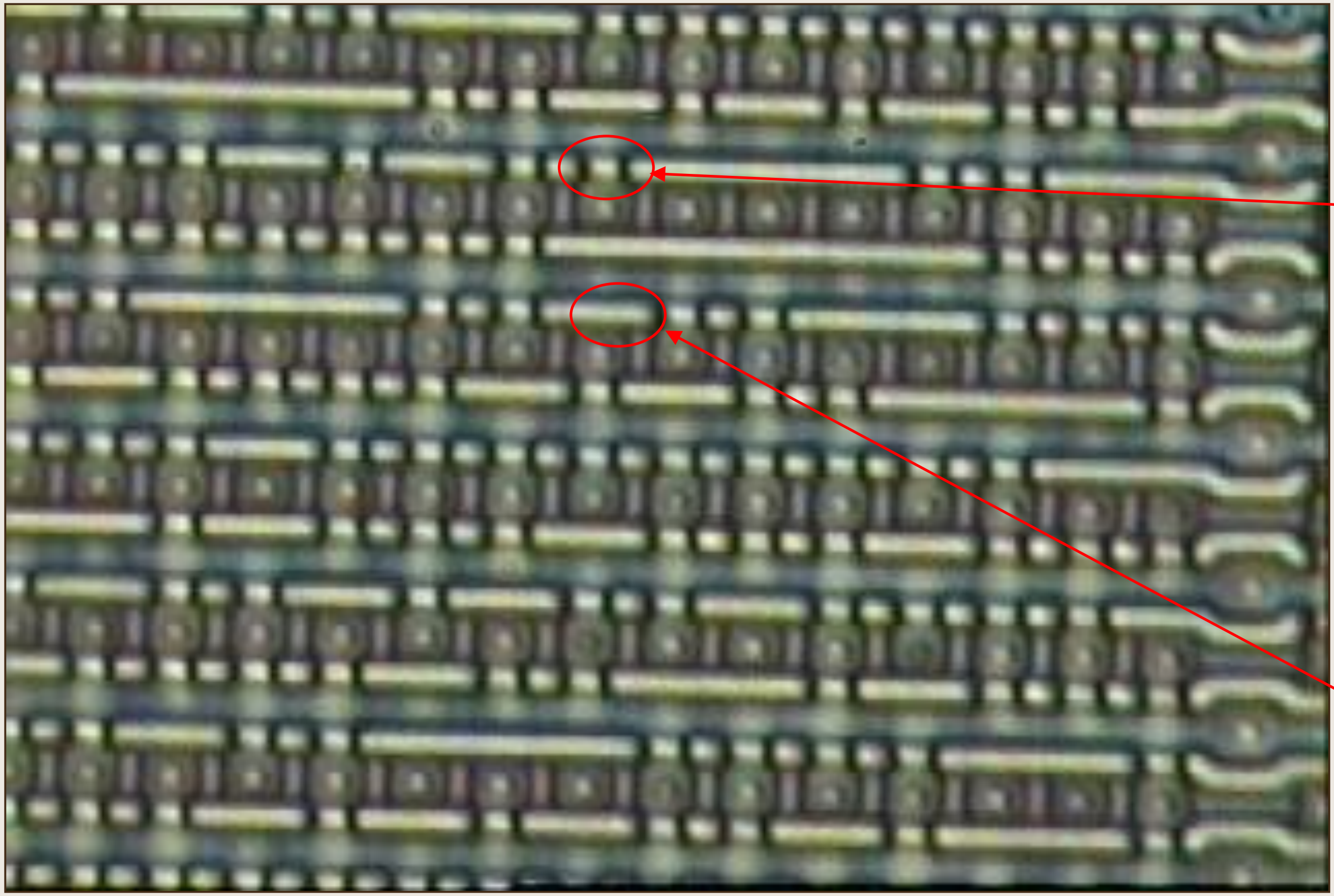


ROM manufacturing

- Physical ROM design
  - physical transistors
  - metal mask ROM
  - ion implantation

- ROM code retrieval
  - reverse engineering of ROM decoders
  - image recognition of ROM cells
  - staining of ion implant ROM

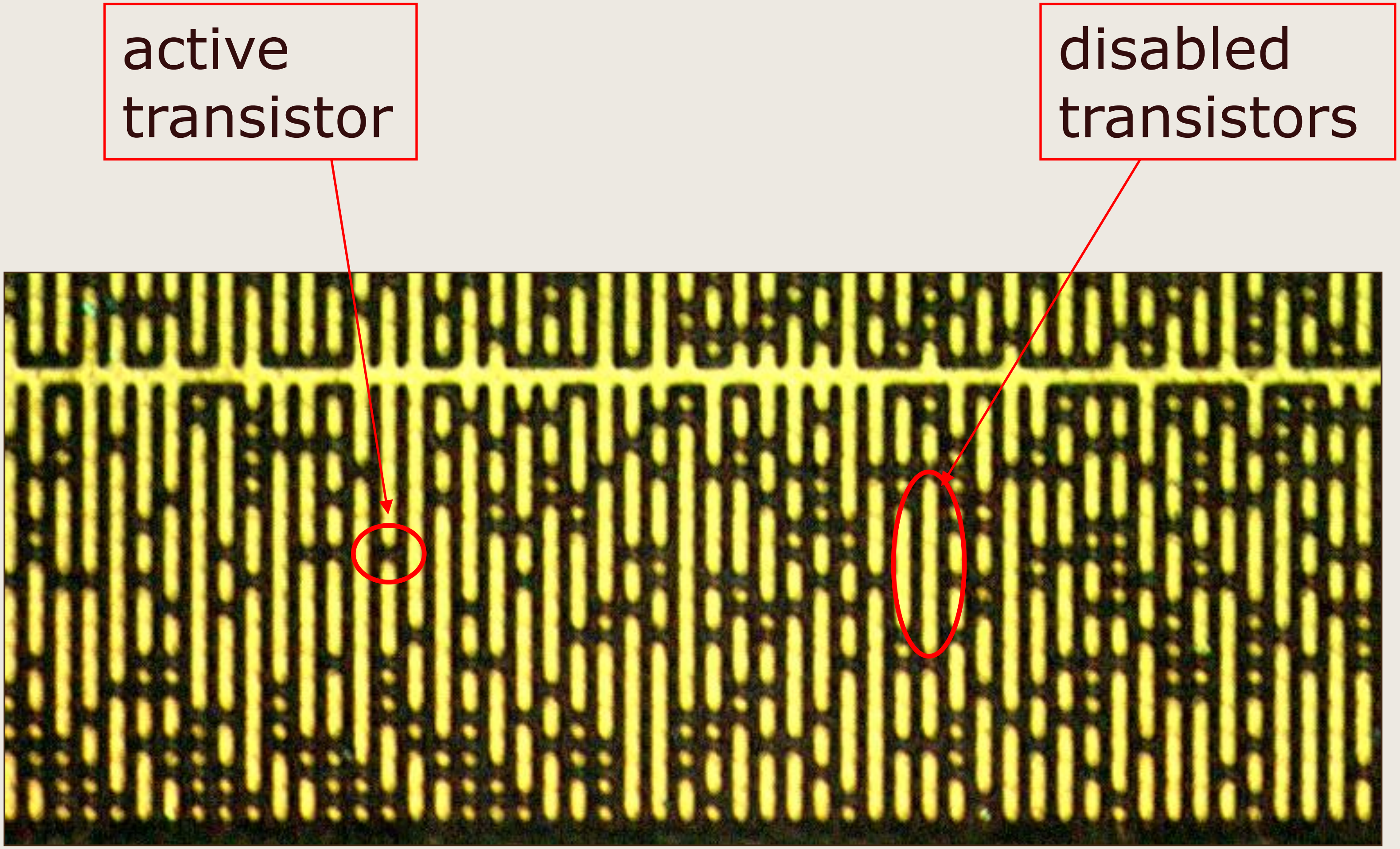
Physical transistors



active transistor

disabled transistor

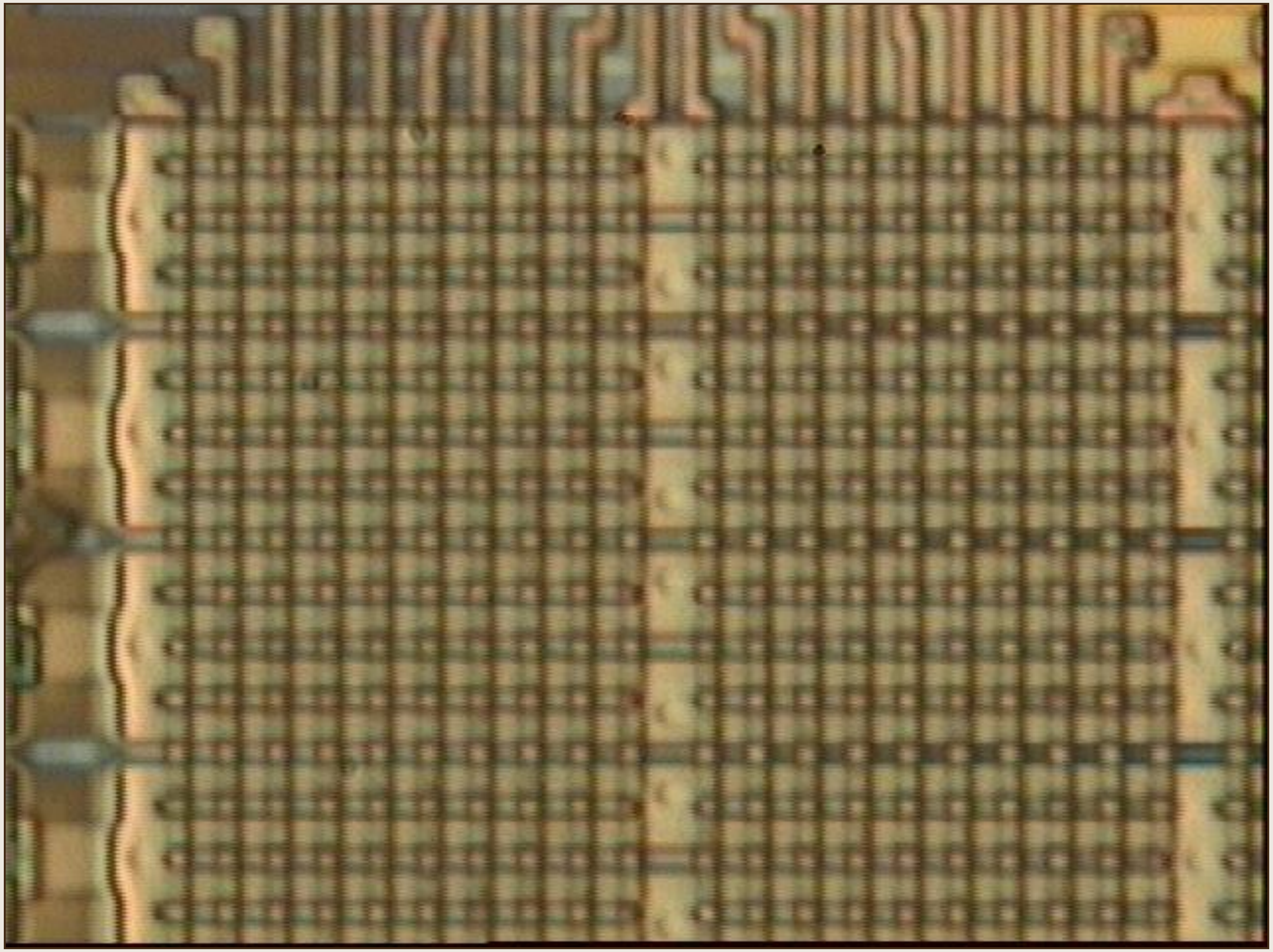
Metal mask ROM



active transistor

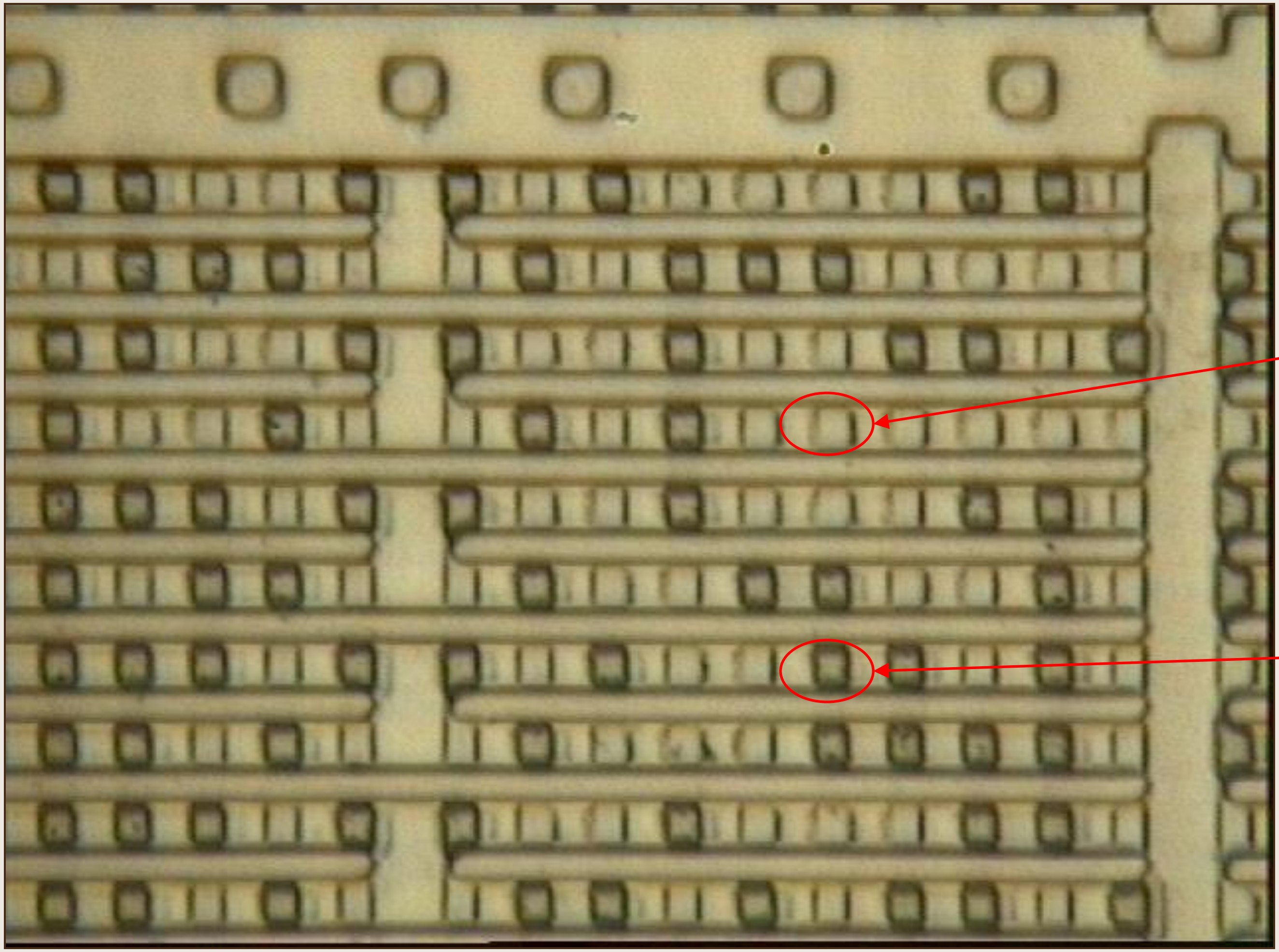
disabled transistors

Ion implantation



No visible difference between cells

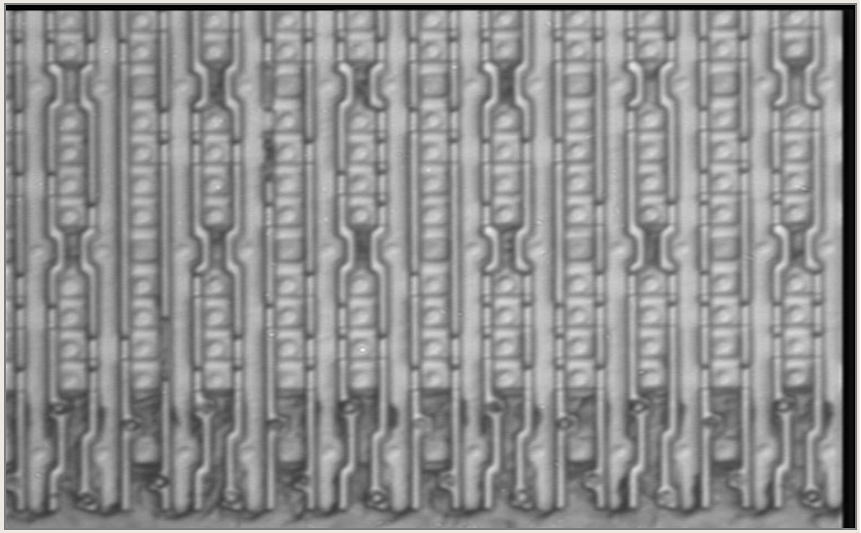
Ion implant ROM after chemical staining

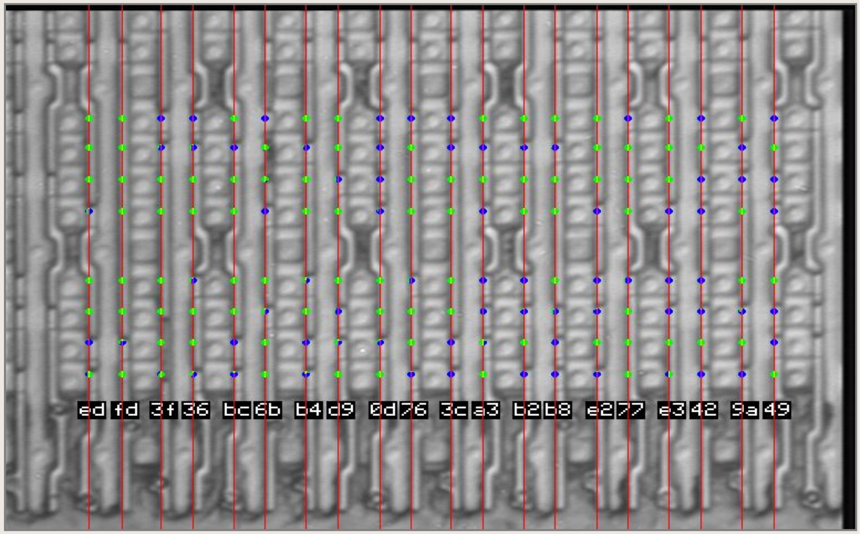


Logical one

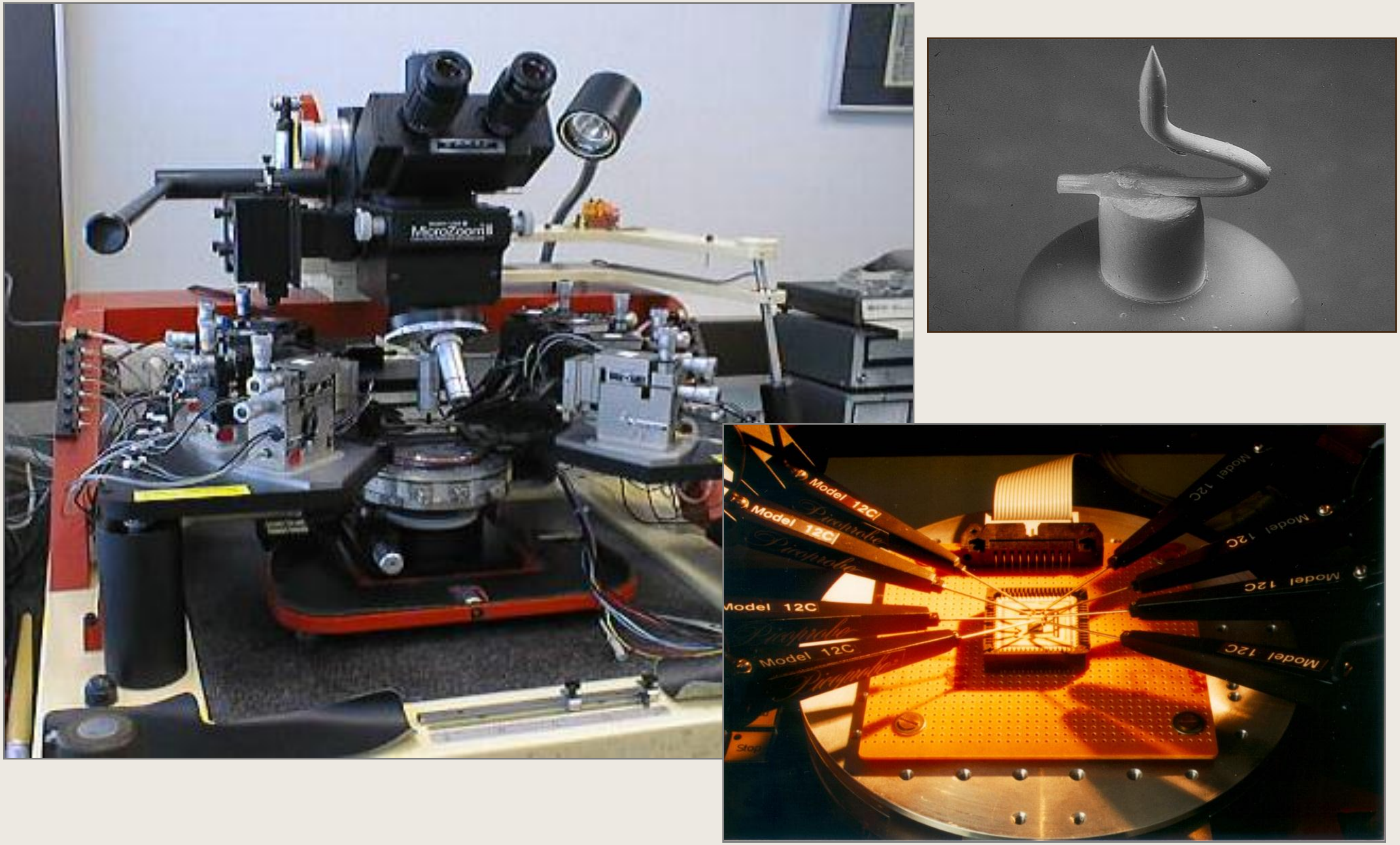
Logical zero

ROM code extraction

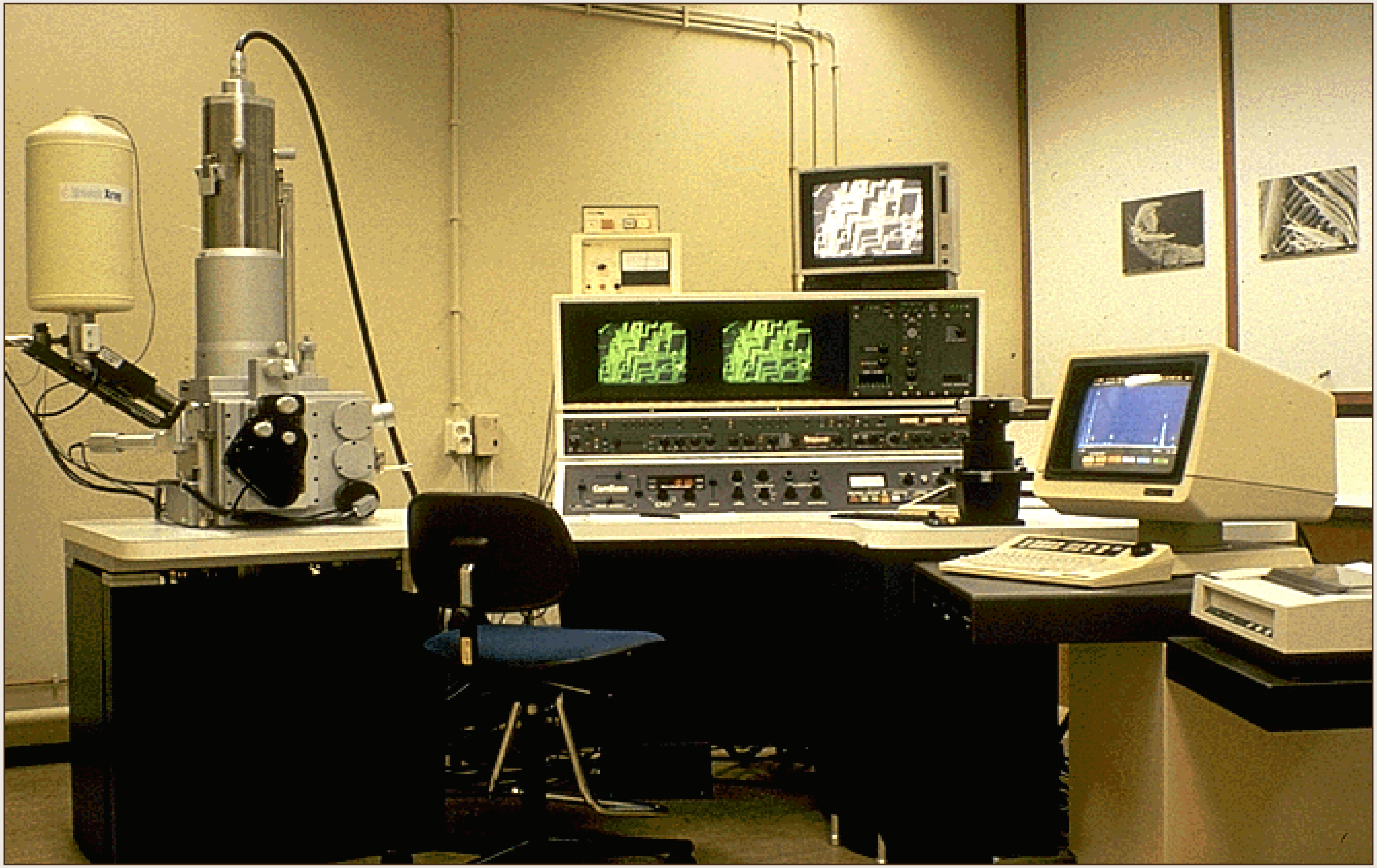




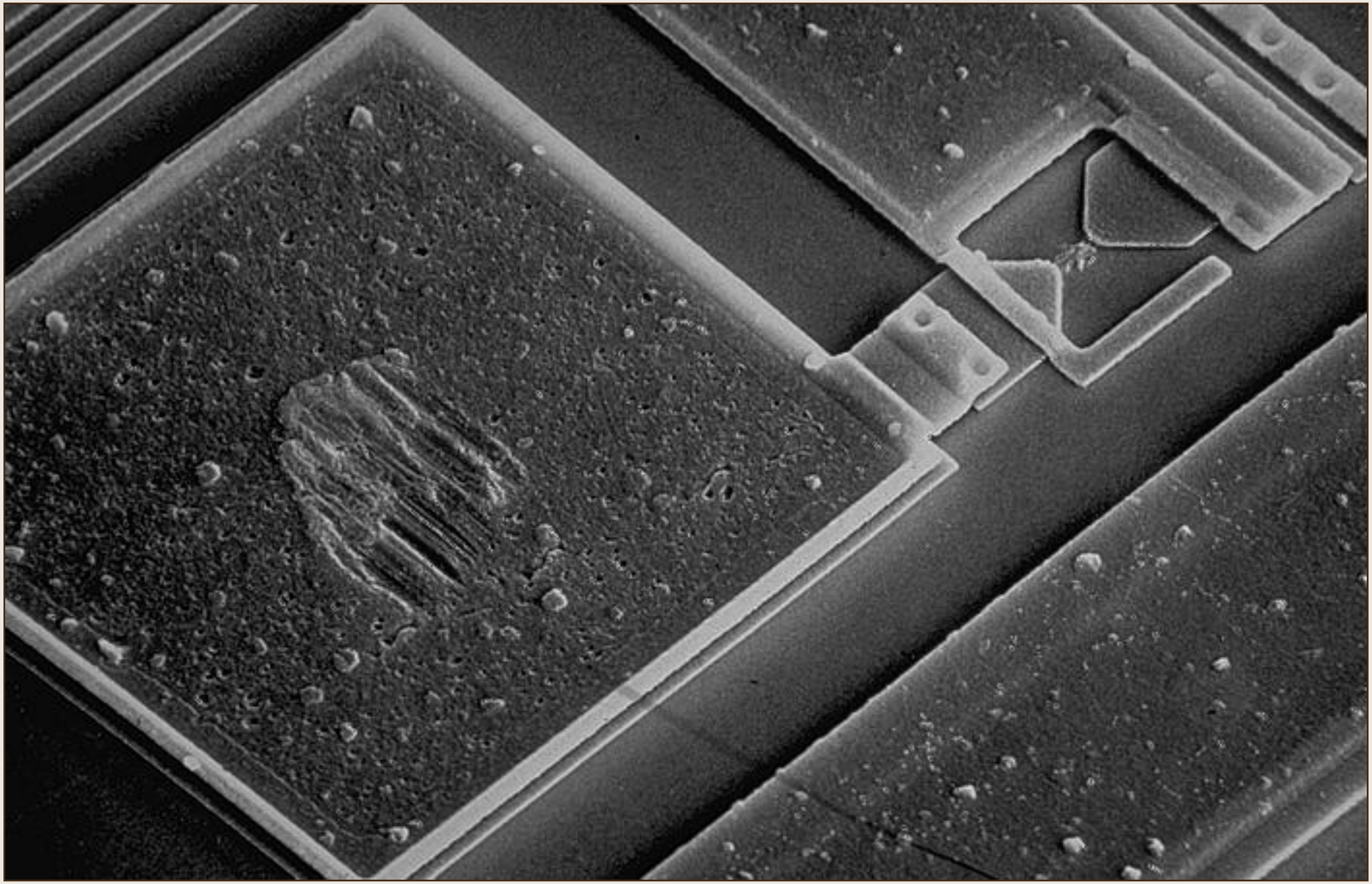
Mechanical probing



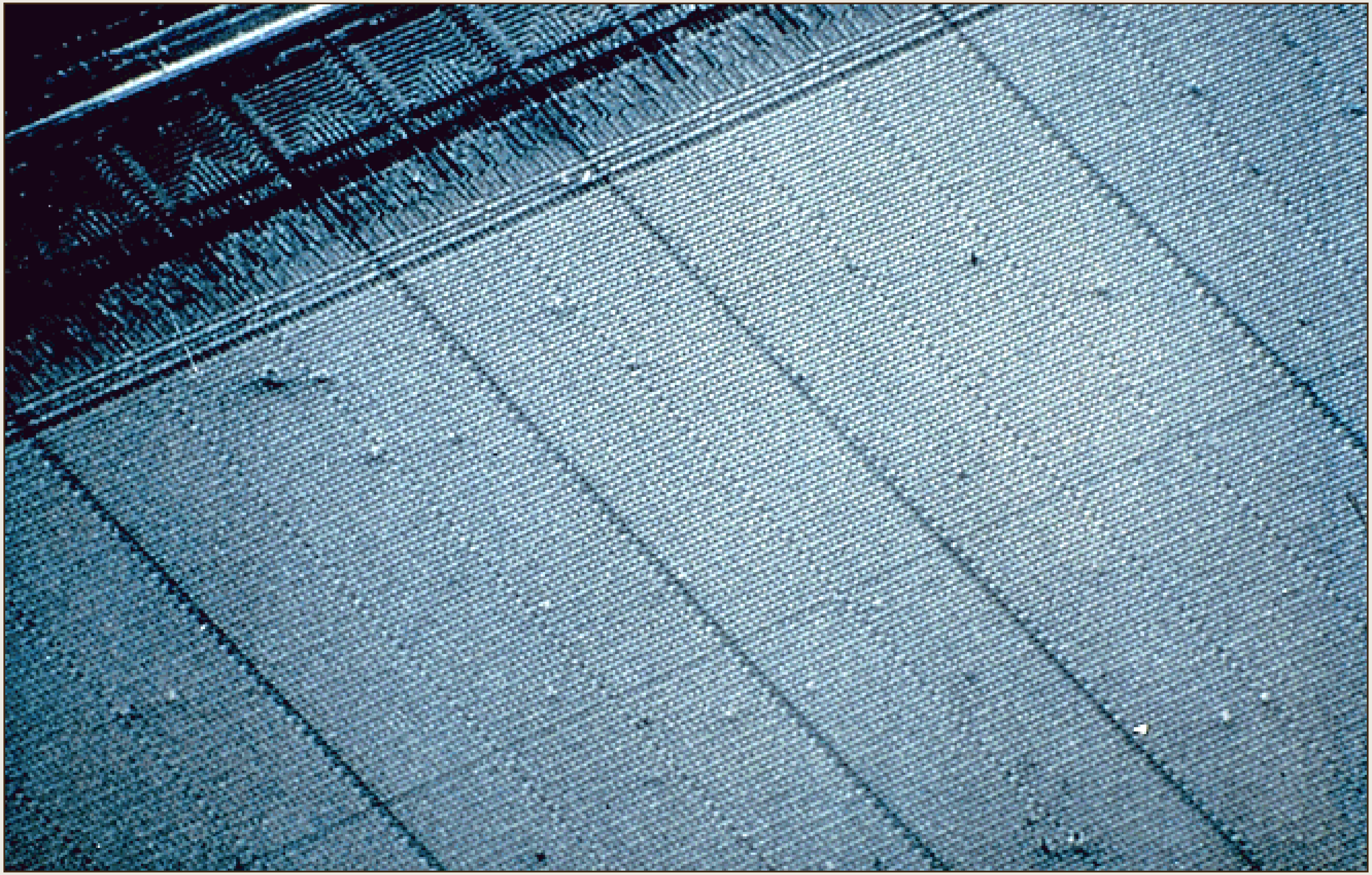
Scanning Electron Microscope



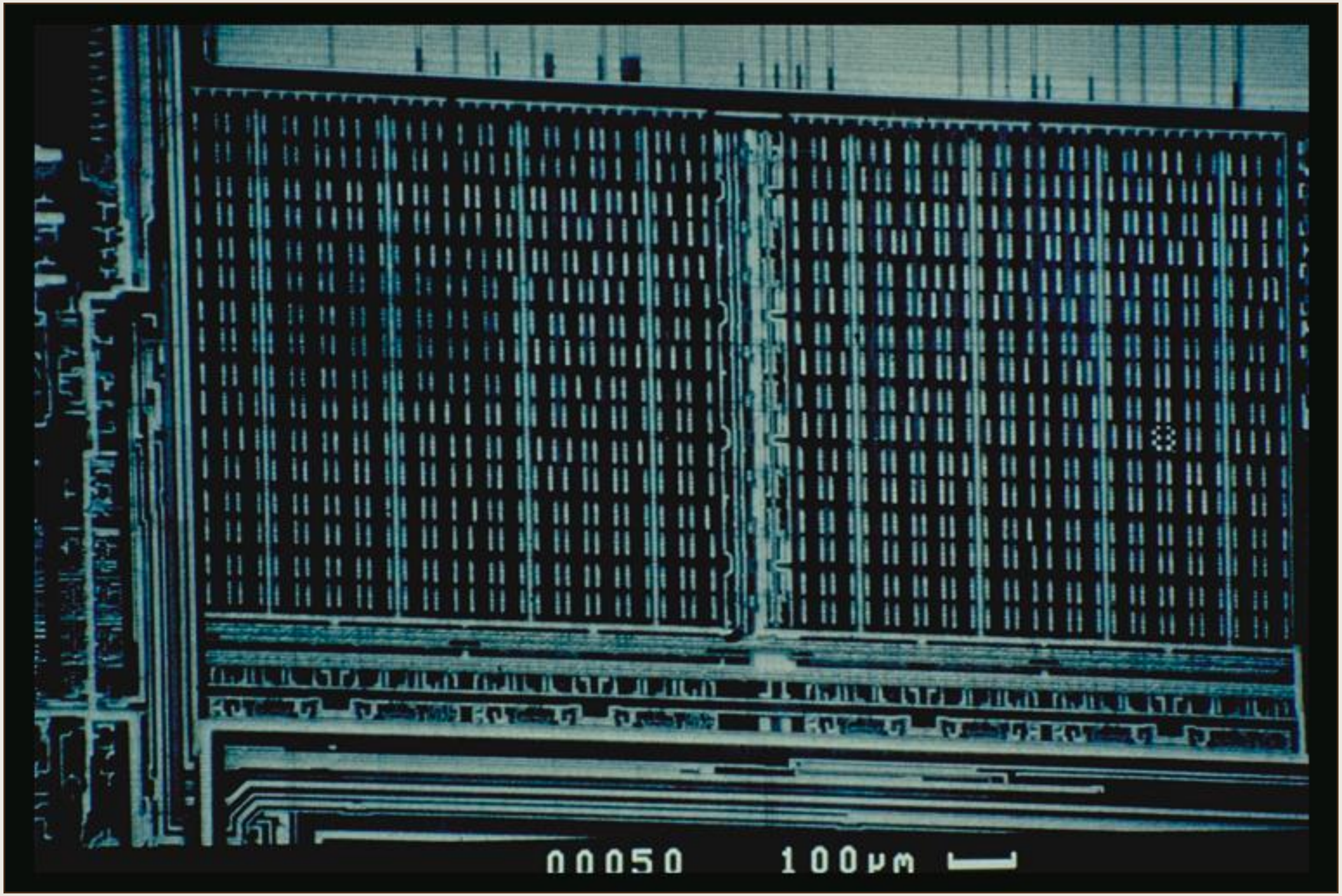
On-chip fuse (blown)



Voltage Contrast



Voltage Contrast: RAM contents



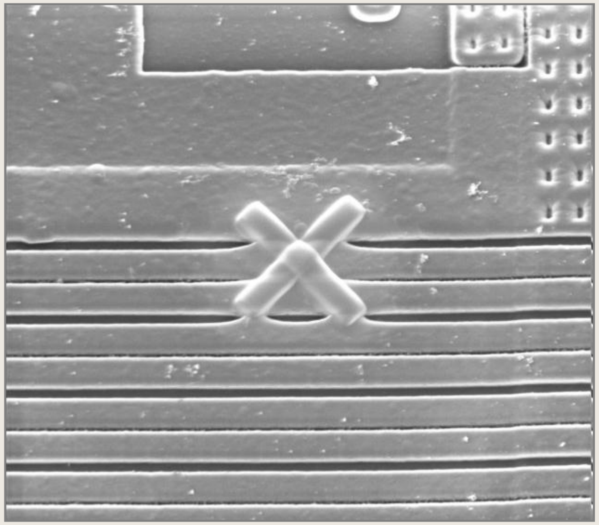
Focused Ion Beam modification

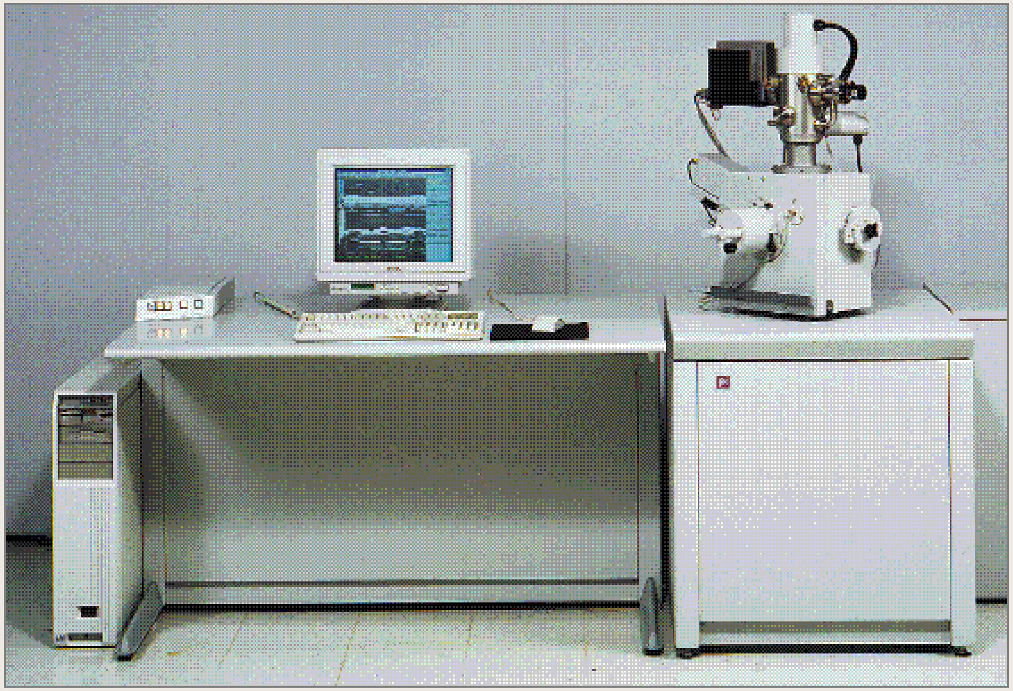
□ Re-route logic

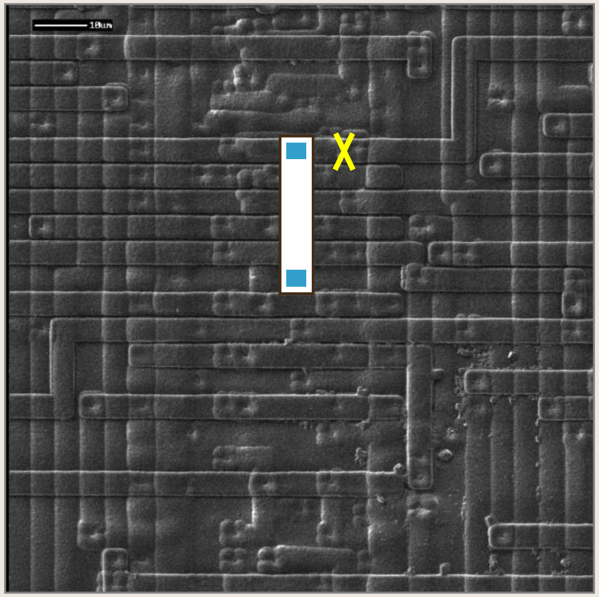
□ Disable sensors (e.g. shield)

□ Make probe pads

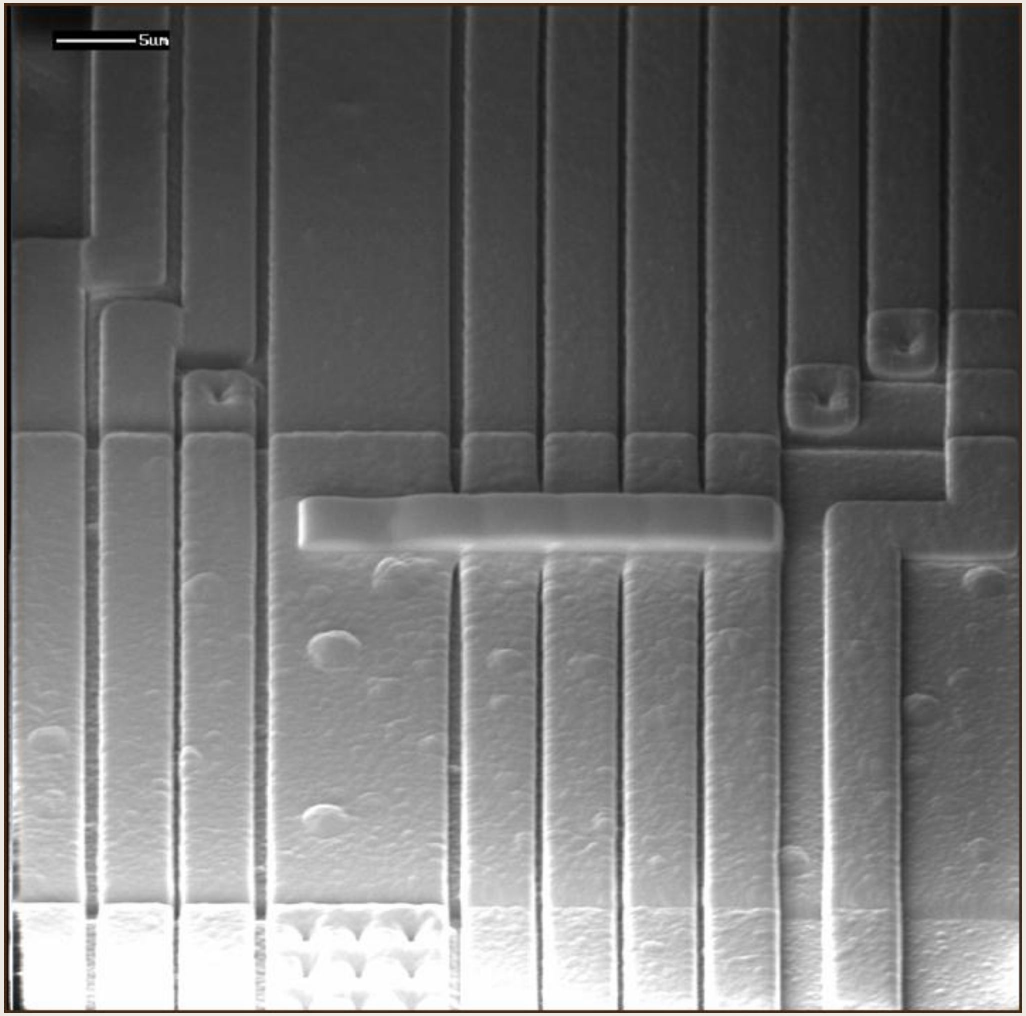
□ Backside FIB edits



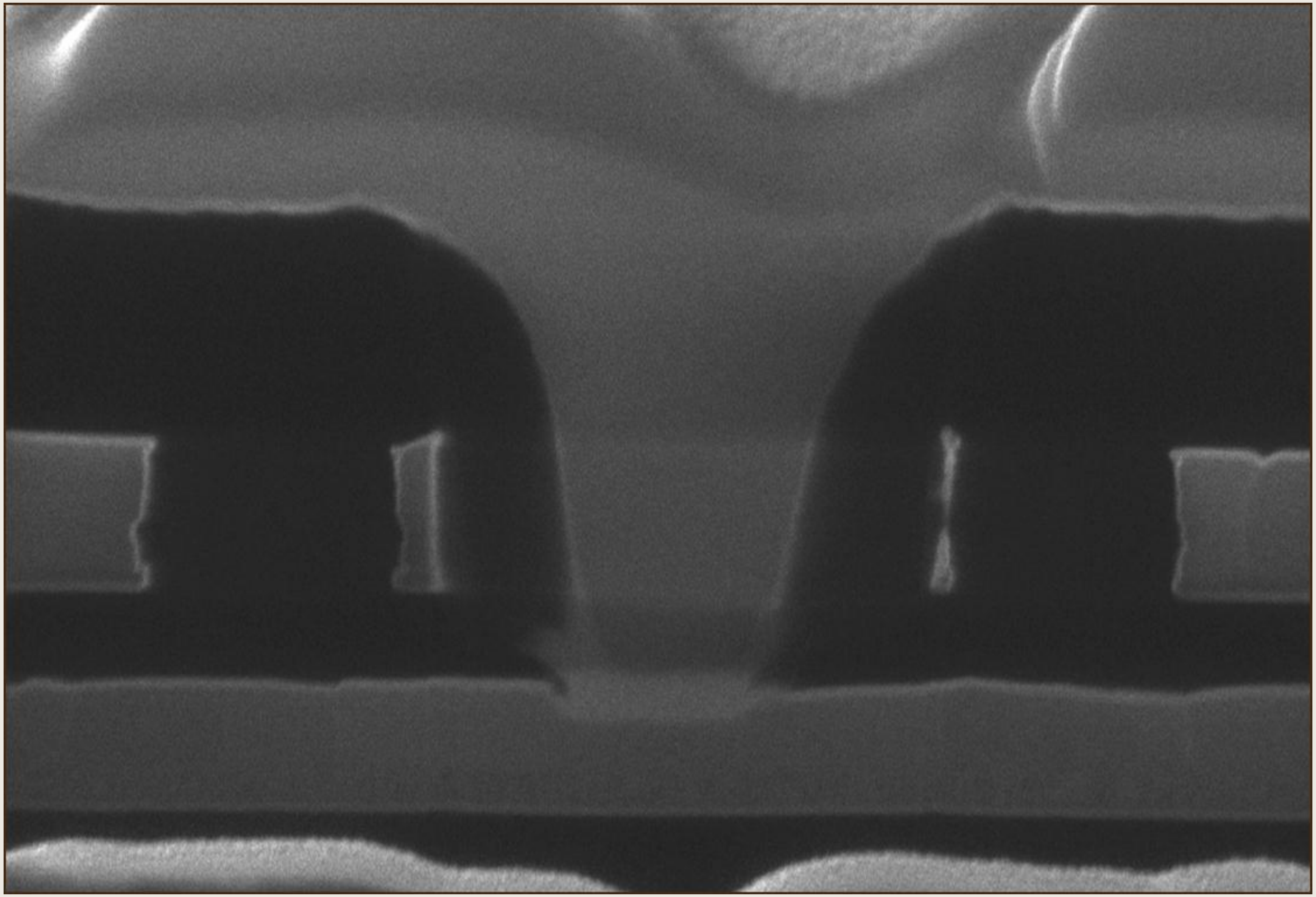




Examples of FIB modifications: circuit edit



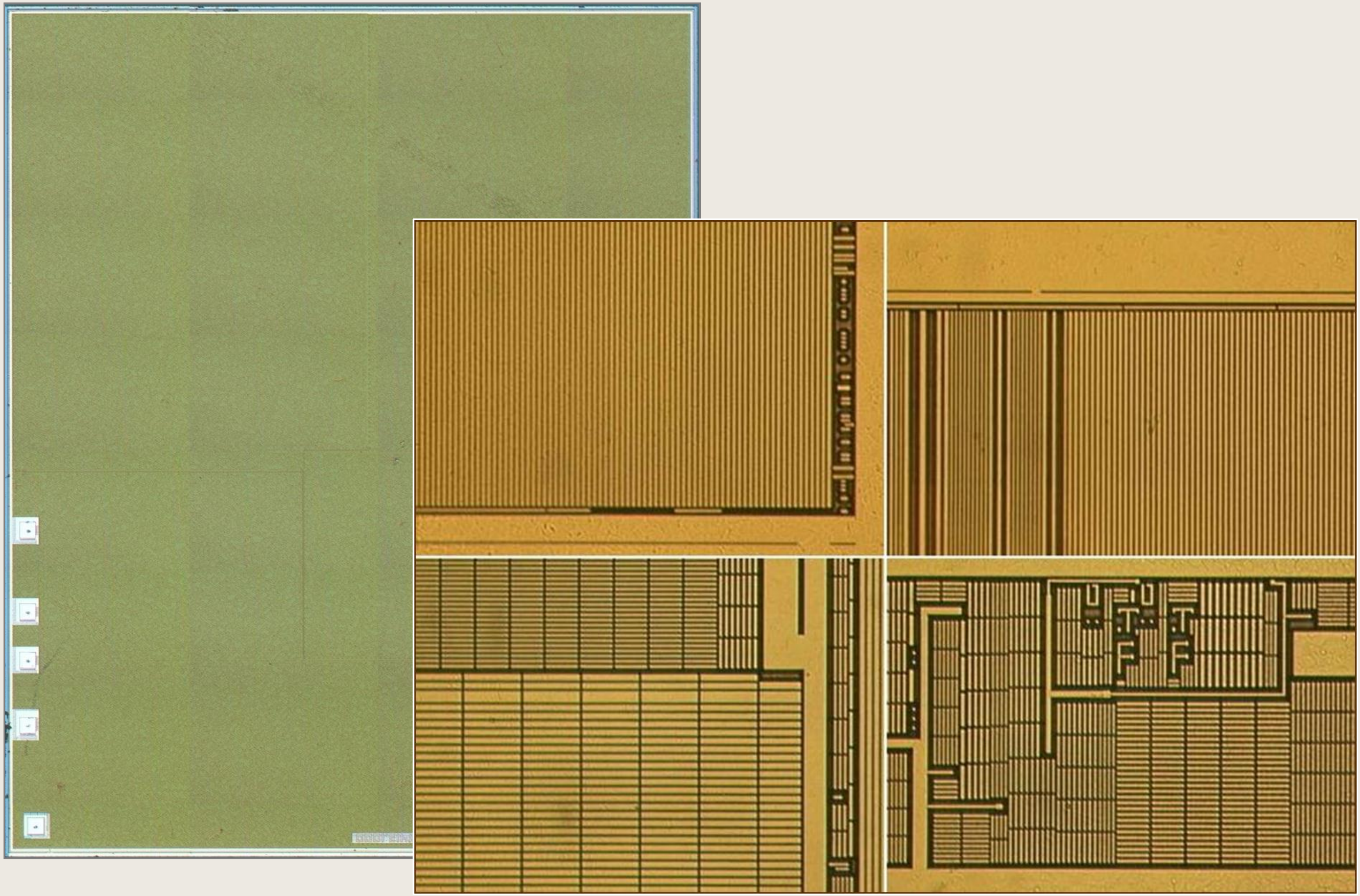
Examples of FIB modifications: access lower layers



State-of-the-art in secure controllers

- Environmental sensors (active shields, light, clock frequency, voltage, glitch, temperature)
- Small feature size (~130nm) and 5-6 metal layers
- High complexity by using glue logic
- Internal encryption of bus and memory data
- Dedicated encryption hardware
- Hardware redundancy
- Countermeasures against perturbation and Side Channel Analysis
- Hardened software and resilient protocols

Physical shielding



Conclusions:
Do we need physical security?

- Overall security is provided by a good combination of:
  - physical security measures
  - logical security measures
  - organizational security measures
- 100% security is never possible
- Secure Cryptographic Devices and smart cards are part of a system
- we need a secure *system* !

Brightsight on the web:

You can find us at:

www.brightsight.com

www.facebook.com/brightsightbv

Did you 👍 this presentation?