

Hardware Security – Smartcards and other Tamper-Resistant Modules

Markus G. Kuhn
Computer Laboratory



UNIVERSITY OF
CAMBRIDGE

<http://www.cl.cam.ac.uk/~mgk25/>

Applications of Tamper Resistant Modules

Security of cryptographic applications is based on secure storage of secret keys and unobservability of computation

Distributed and mobile applications allow attacker full physical access to hardware over extended period of time

- pay-TV access control
- electronic purses
- financial transaction terminals
- software copy protection
- prepayment meters
- anti-theft protection
- authentic telemetry
- protection of algorithms
- cellular phones
- ...

Classes of Attacks on Security Modules

Hardware Emulation

Replace a component of a system by an in-circuit simulator that helps to circumvent access control mechanisms in order to access protected services and secret data

Microprobing

Open the package of a security module and observe or modify the internal communication lines where secrets are transmitted

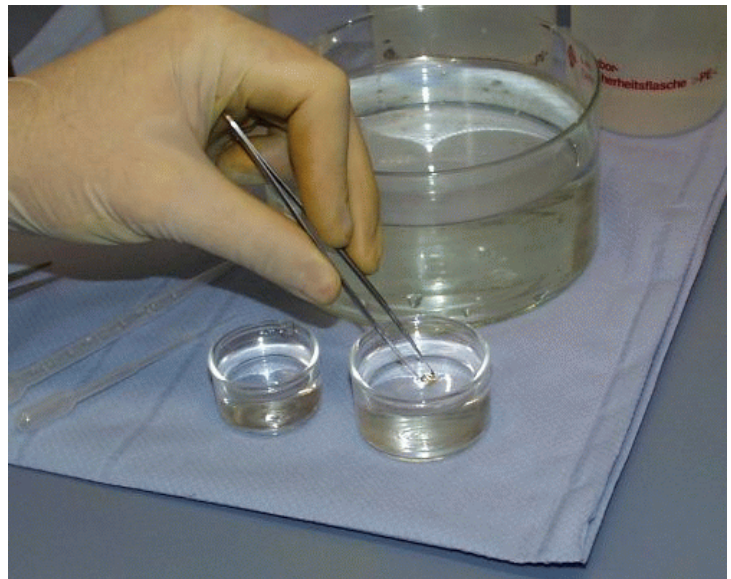
Eavesdropping

Without opening the package, try to get access to protected information by analyzing compromising signals in emanated electromagnetic radiation, supply current fluctuations, leakage currents on signal lines, and protocol timing

Fault Generation

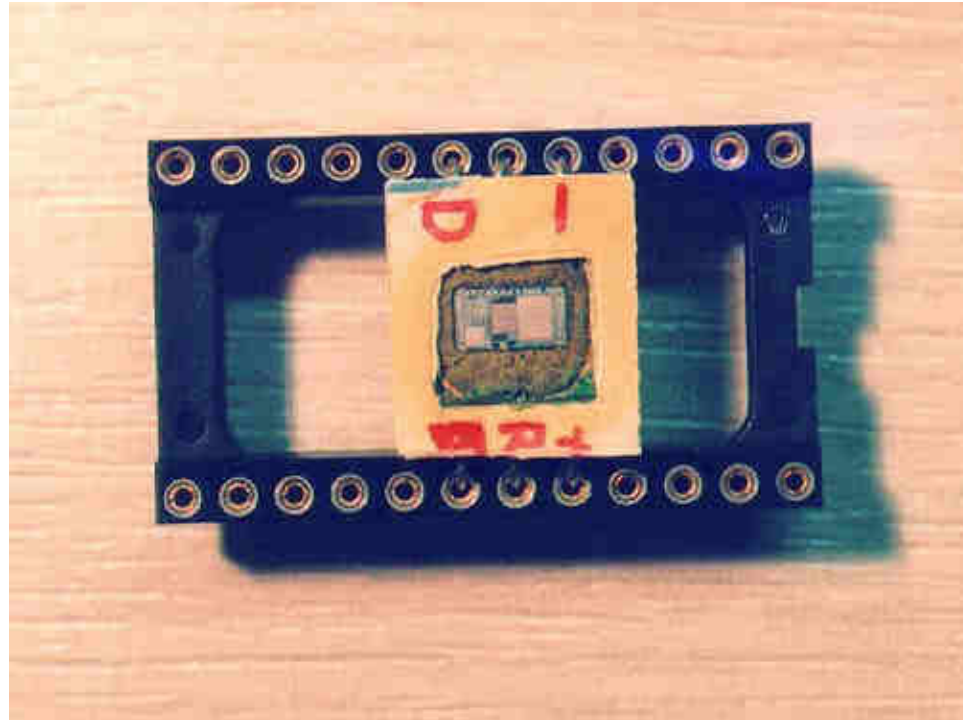
Provoke malfunctions by operating the device under environmental stress conditions such as high/low temperature, supply voltage variations and spikes, clock phase jumps, ionising radiation, protocol violations, partial resets, etc.

Preparation I: Depackaging the Processor



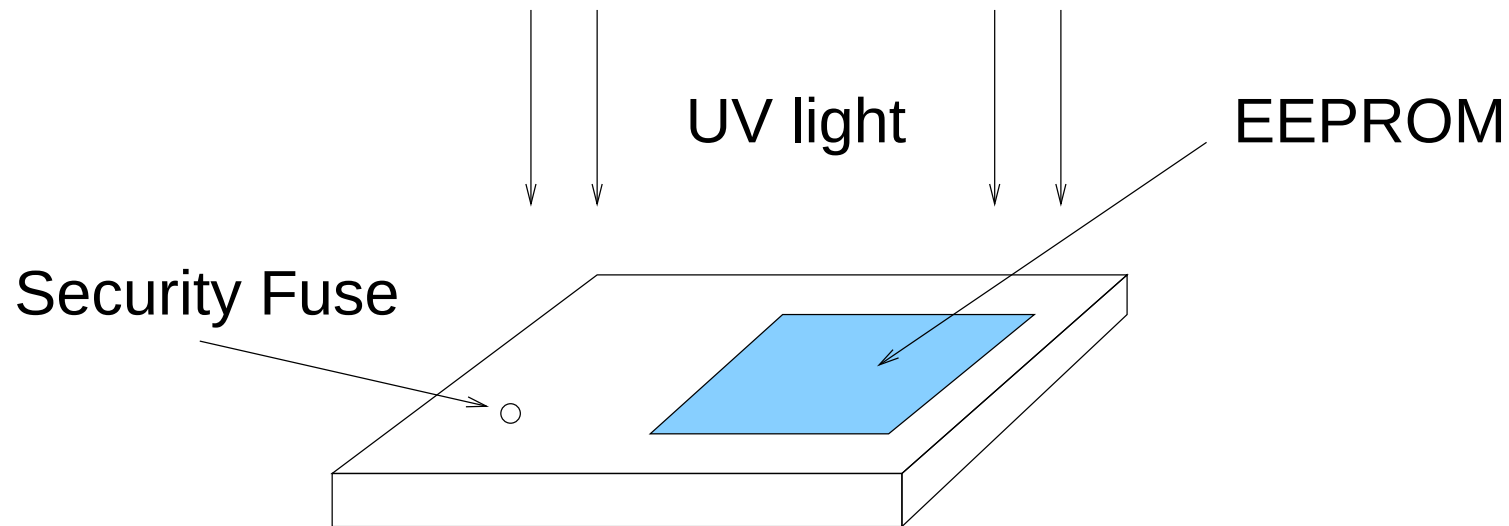
- 1) Heat up card plastic, bend it, and remove chip module
- 2) Dissolve package in 60 °C fuming nitric acid, then wash in acetone, deionized water, and finally isopropanol. The etching should be carried out under very dry conditions.

Getting Access to the Die Surface in Plastic Chips and Smartcards



- 1) Remove covering plastic manually
- 2) Put with a pipette a few drops fuming nitric acid ($>98\%$ HNO_3) on remaining plastic
- 3) Etching process can be accelerated by heating up chip and acid with IR radiator
- 4) Wash away acid and dissolved plastic with acetone
- 5) Repeat from step 2 until die surface is fully exposed

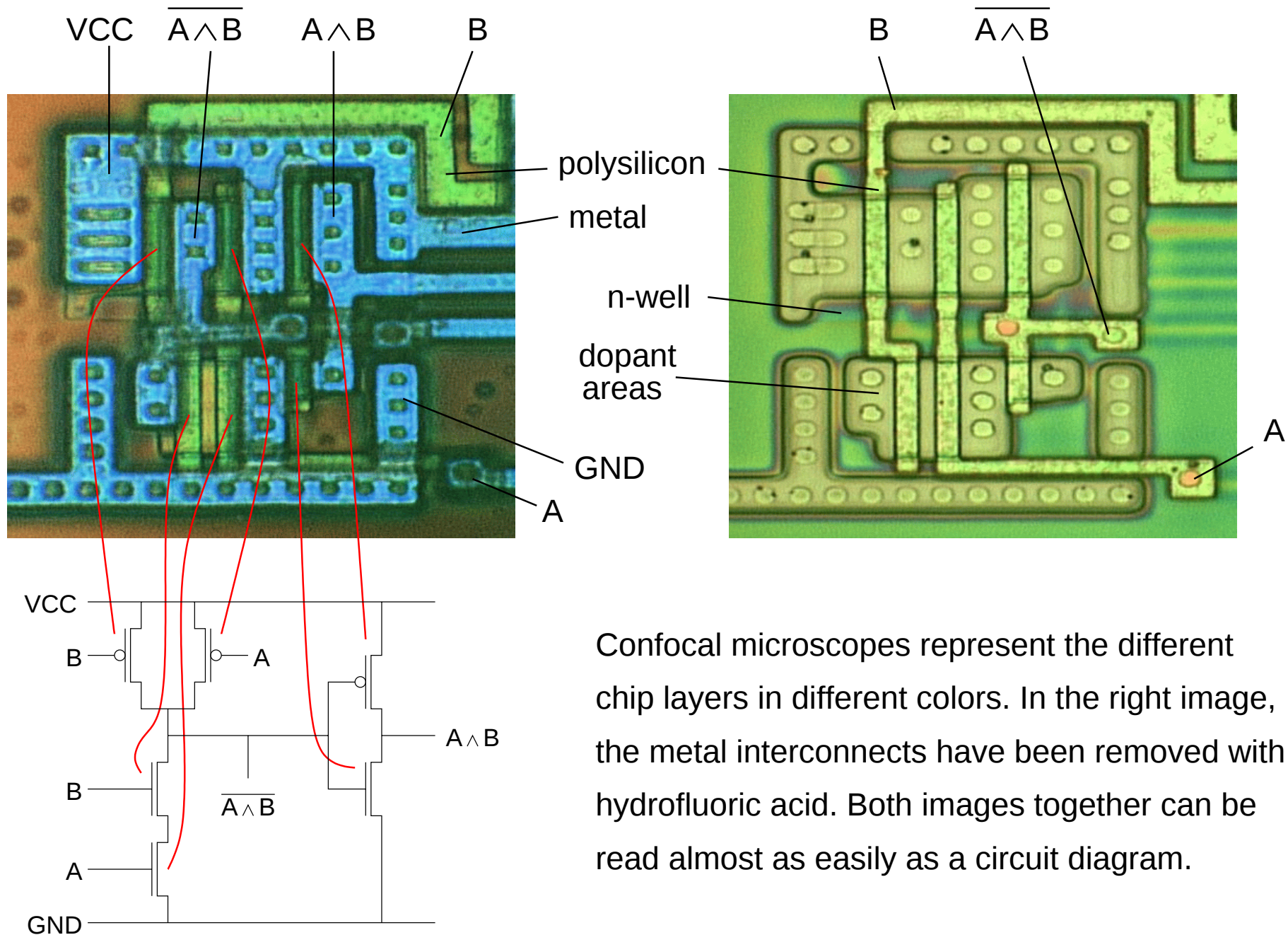
UV Read-out of Standard Microcontrollers



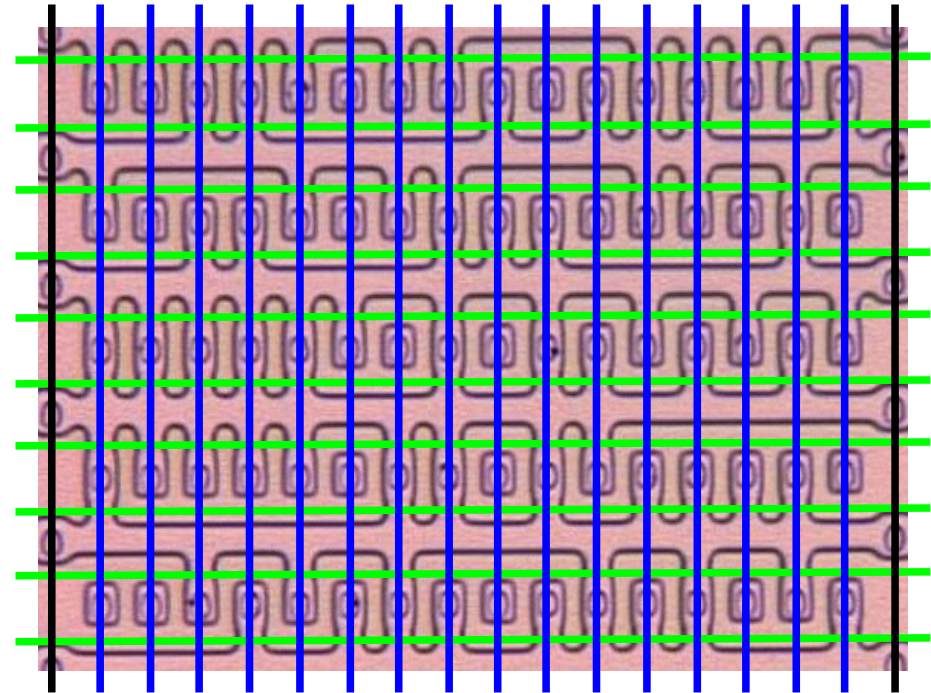
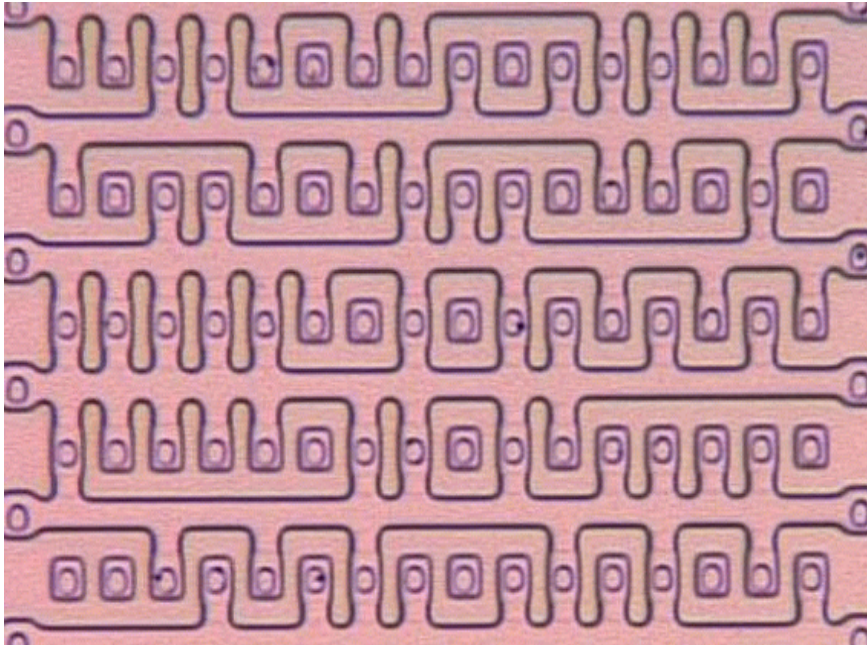
Many microcontrollers have an EEPROM security fuse located outside the EEPROM program memory.

- Open chip package
- Cover program memory with opaque material
- Reset security fuse in UV EPROM eraser
- Access memory with program/verify commands

Optical Reverse-Engineering of VLSI Circuits



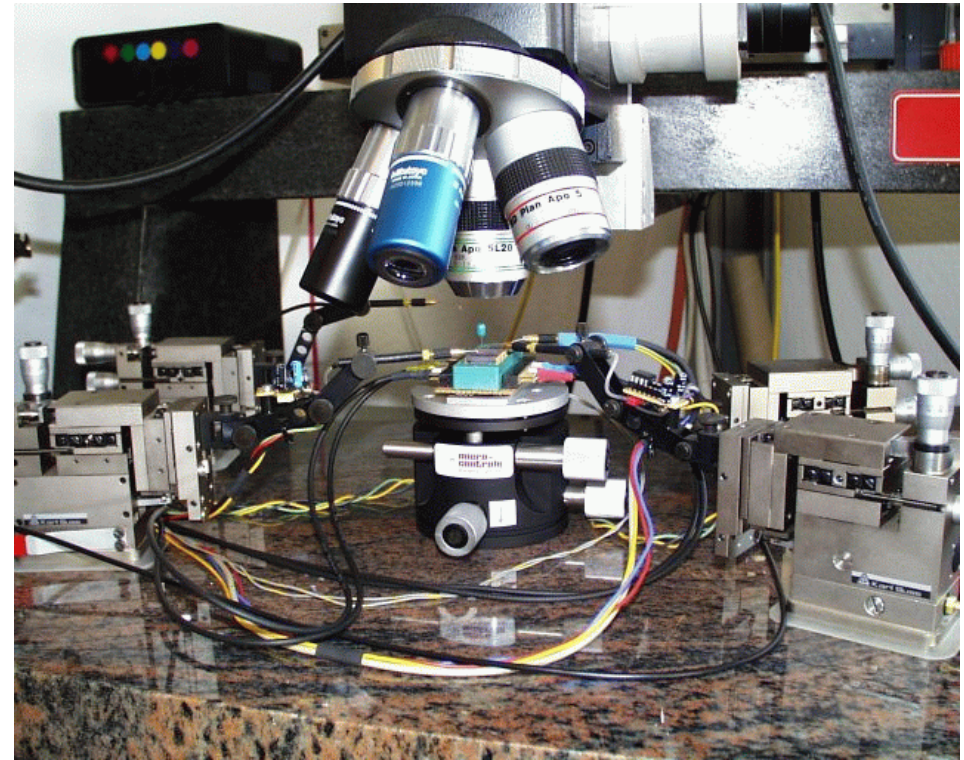
Optical Access to Diffusion Layer ROM Content



After all covering layers including the surrounding field oxide have been removed with hydrofluoric acid, the shape of the now visible diffusion areas will reveal the ROM content (here 16x10 bits).

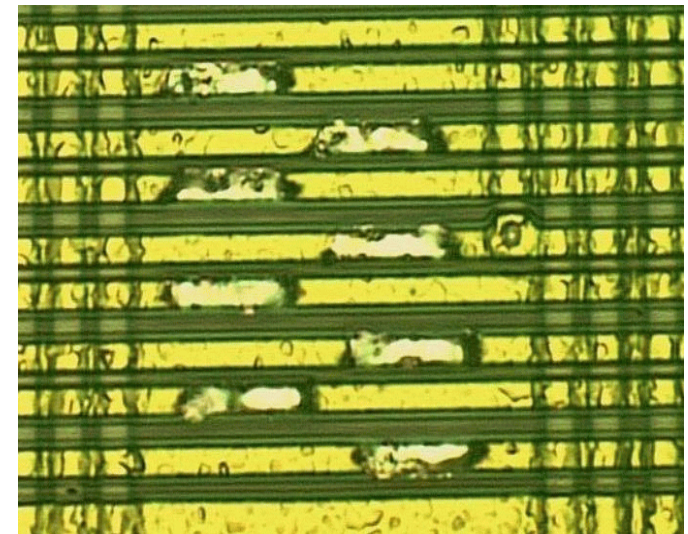
- polysilicon row access line
- metal column access line
- ground connection

Access to CPU Bus via Laser Depassivation and Microprobing

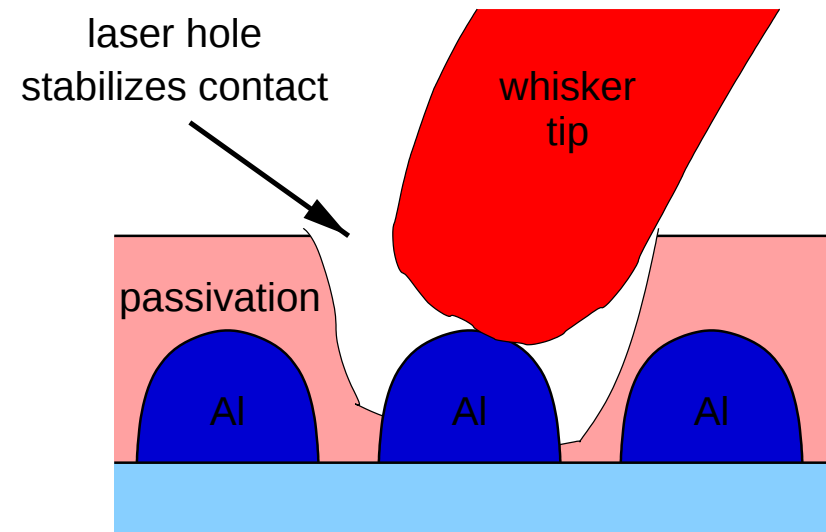
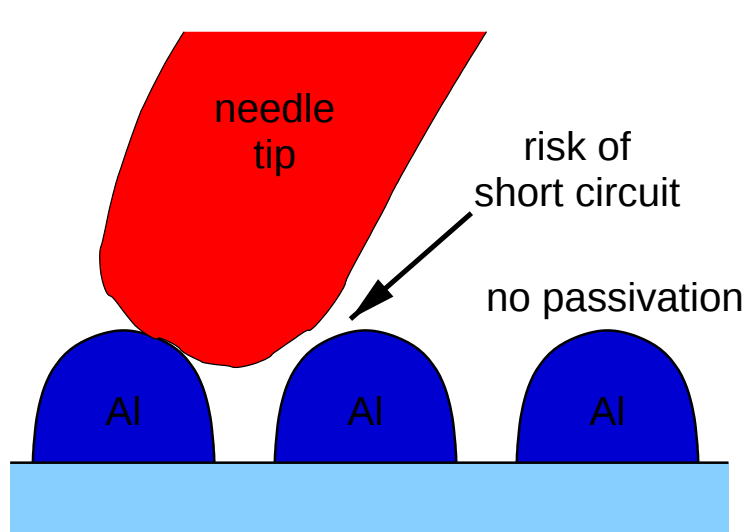
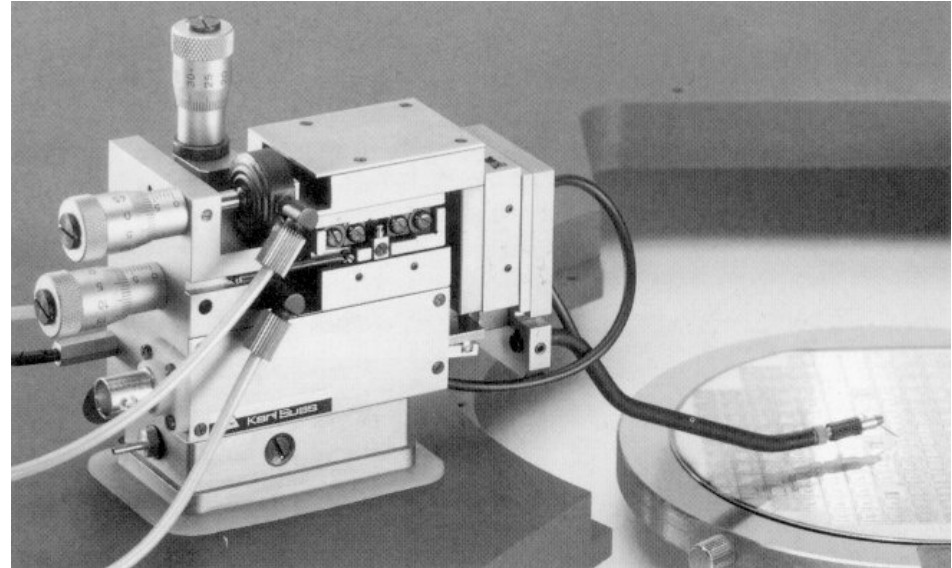
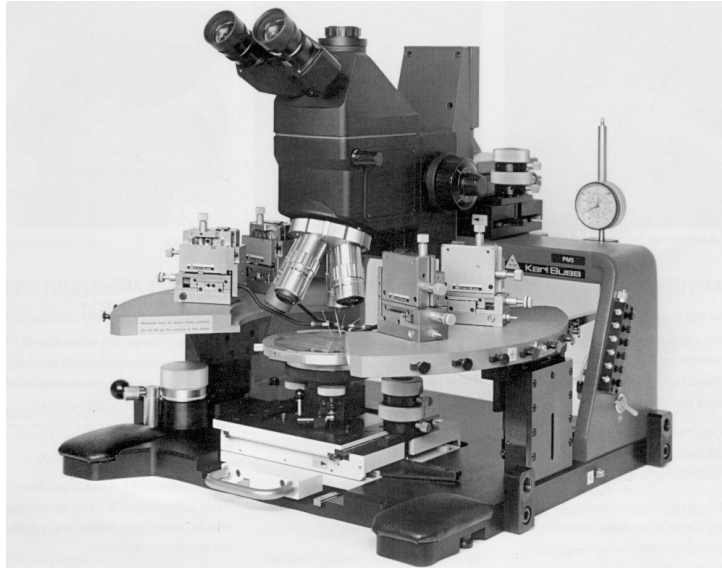


Top: A complete microprobing station consisting of a microscope (Mitutoyo FS-60), laser cutter (New Wave QuikLaze), four micropositioners (Karl Suss), CCD camera, PC with DSP card for card protocol interface handling and data acquisition, oscilloscope, pattern generator, power supply, logic analyzer, etc. Right: Eight depassivated data bus lines.

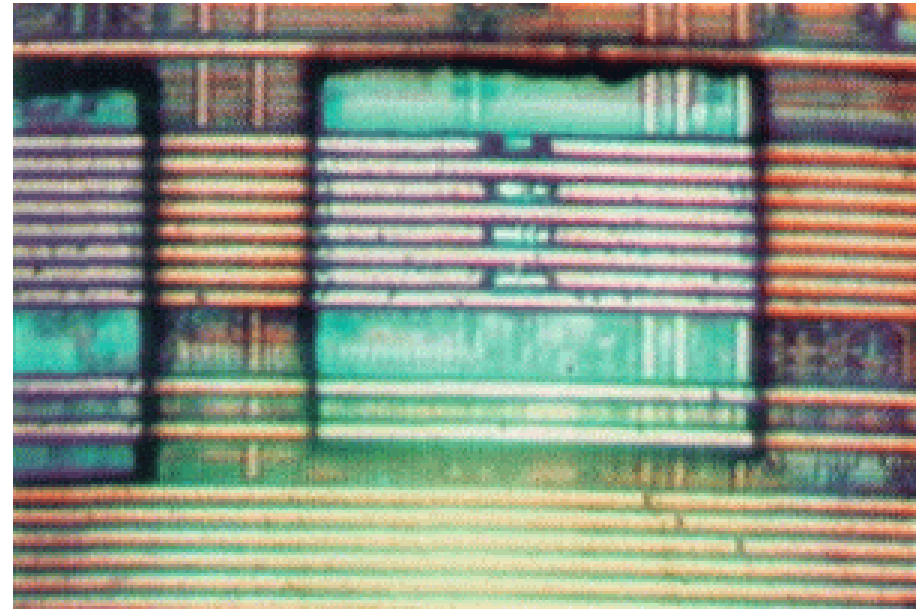
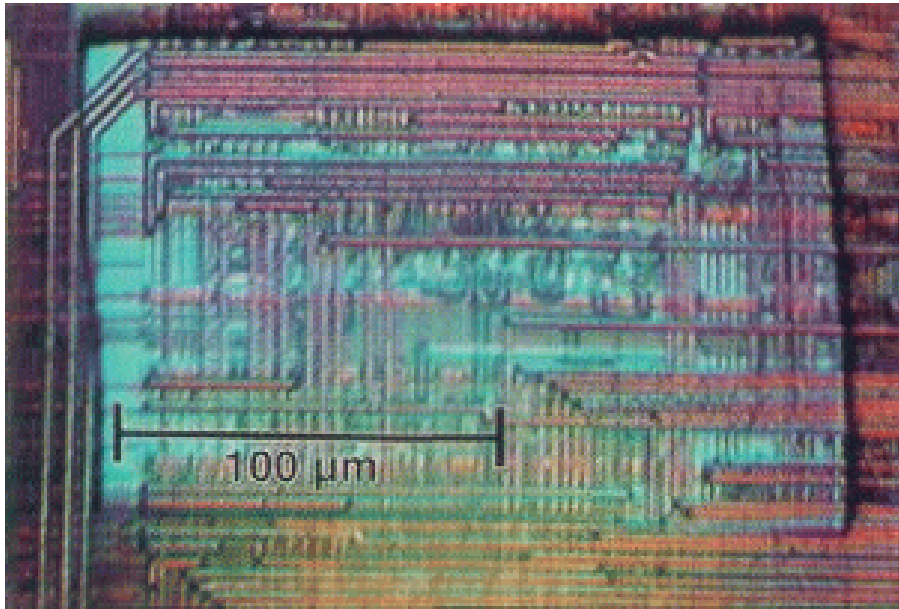
Photos: ADSR



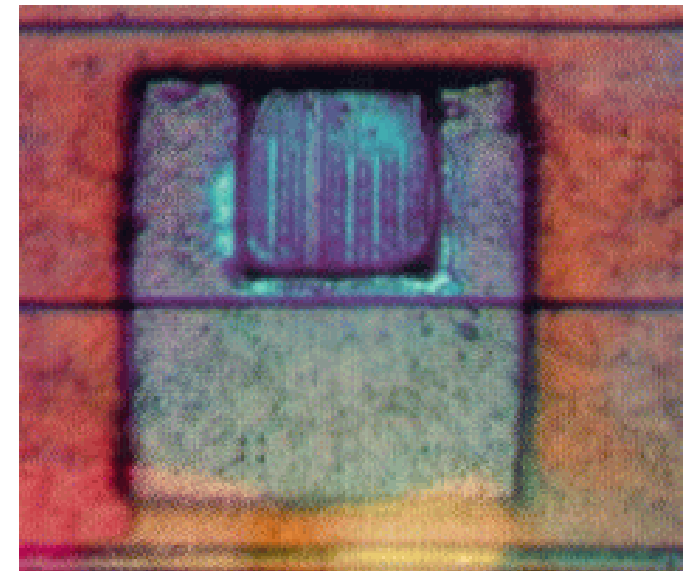
Practical Submicron Microprobing



Laser cutter as a powerful reverse engineering tool



- Local removal of passivation layer with $<1\ \mu\text{m}$ precision (355 nm UV light)
- Removal of oxide (532 nm green light)
- Exposure of lower metal layers for probing
- Cuts in metal and polysilicon lines (532 nm)
- Order of magnitude less expensive than FIB



Photos: New Wave Research

Microprobing Access to All Memory Locations

Passively monitoring and recording all memory-bus accesses might not be sufficient to attack all applications. Carefully designed smartcard software makes it difficult to trigger memory accesses to all secrets in a laboratory.

- Card software that calculates a full memory checksum after each reset simplifies attacks considerably!

Solution for Attacker:

Abuse existing processor hardware as an address generator that accesses all memory locations predictably. A single probing needle can now capture all memory values, probing one bus line at a time.

Options:

- Disable instruction decoder, such that no JMP/CALL/RET/HALT instructions are executed (preferably only NOP-like instructions should be allowed).
- Disable program-counter load gate

In many smartcard processors, this can be accomplished with just a single probe!

Restricted Program Counter

A standard program-counter mechanism is too easily abused as an address-sequence generator. Tamper-resistant design of the instruction decoder is difficult. Watchdog circuitry requires many transistors and simple forms are also easily disabled.

Solution:

- Replace the normal program counter (e.g., 16 bit) by a combination of a full-size segment register S and a short (e.g., 7 bit) offset register O .
- Instructions are fetched from address $S+O$.
- Only O is automatically incremented after every instruction. An overflow of O will halt the processor.
- A jump to address X is performed by loading X into S and setting O to zero.
- Unconditional jump commands must be less than 128 bytes apart, which an assembler preprocessor used by the developer can ensure automatically.

Now, no simple FIB edit can cause the program counter to cover all addresses.

Destruction of Test Circuitry

Attackers and test engineers share similar interests. Both need easy access to the on-chip bus lines with as few probes as possible.

Commonly used test circuitry:

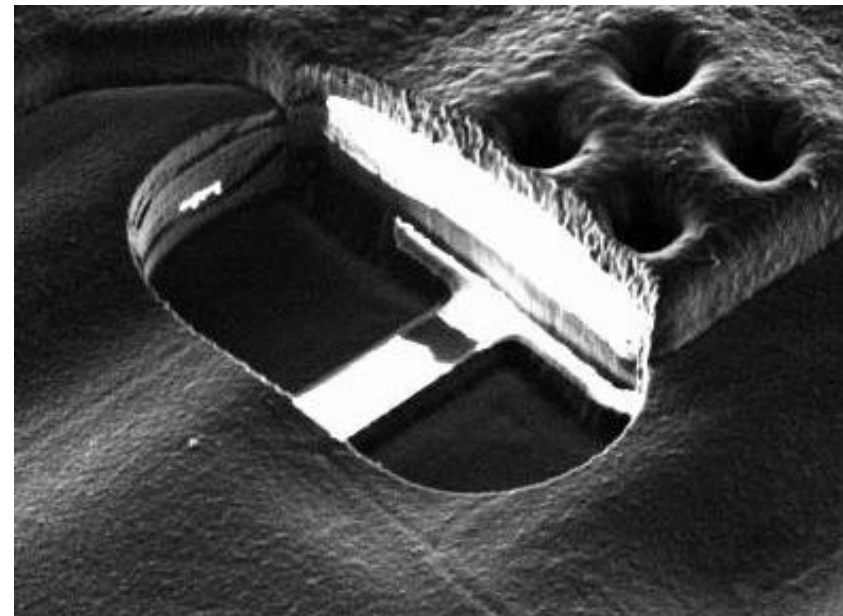
- Parallel/serial converters for full bus
- Full bus available on large probing pads

Pads usually disabled by blowing a poly fuse, but can easily be reconnected via FIB.

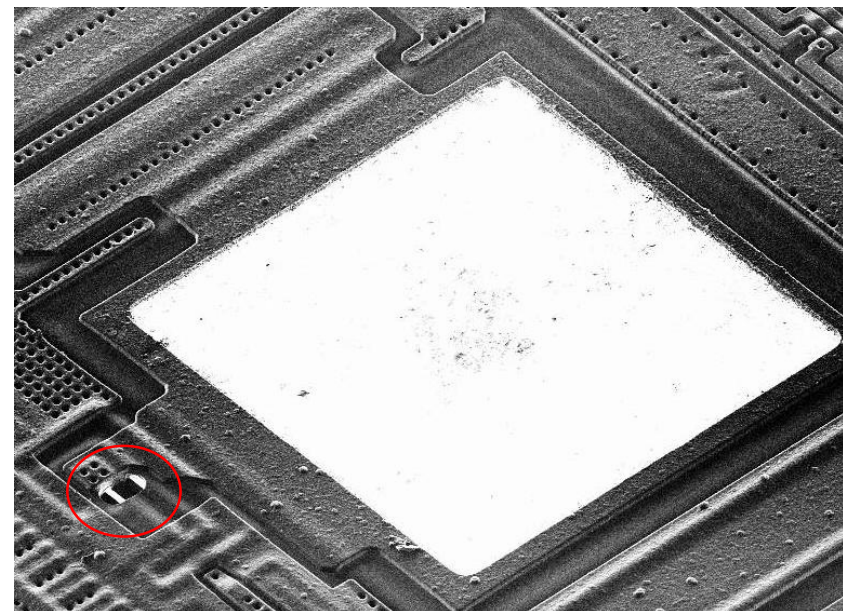
Solution:

Test circuitry must not only be disabled by blowing fuses. It must be structurally destroyed.

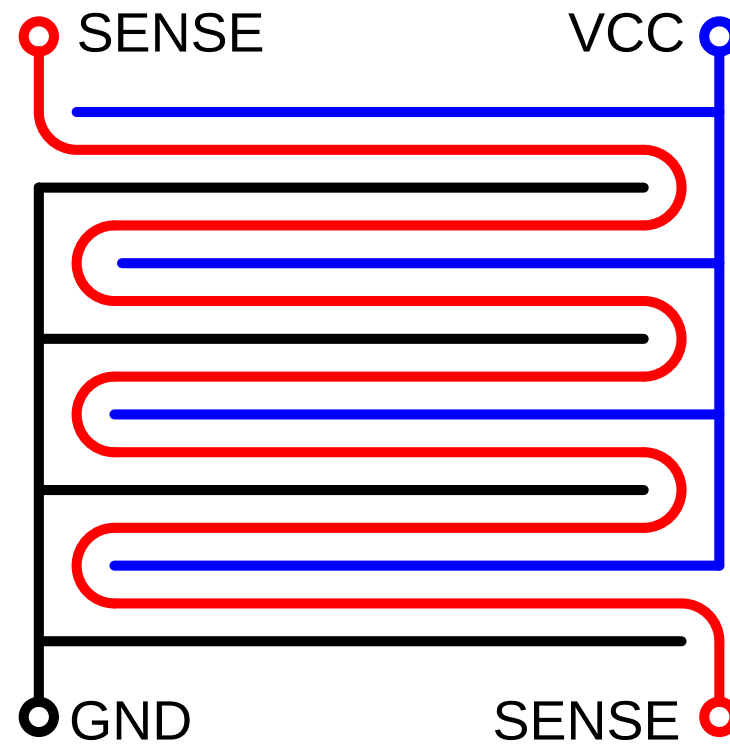
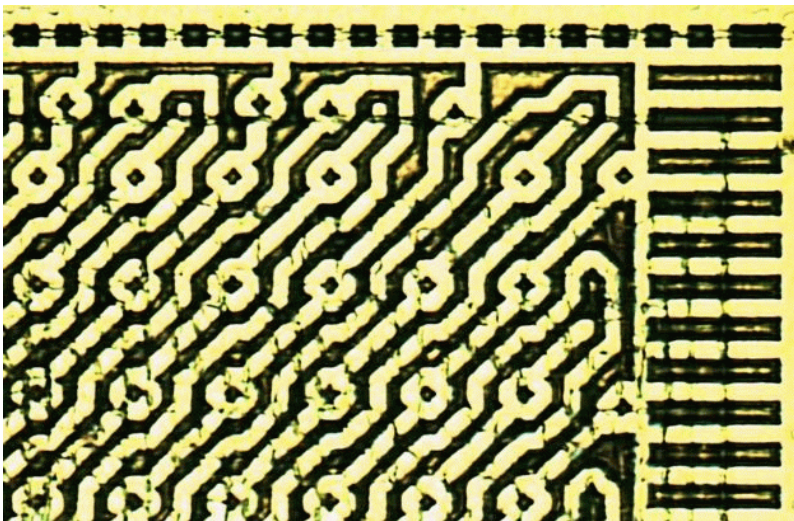
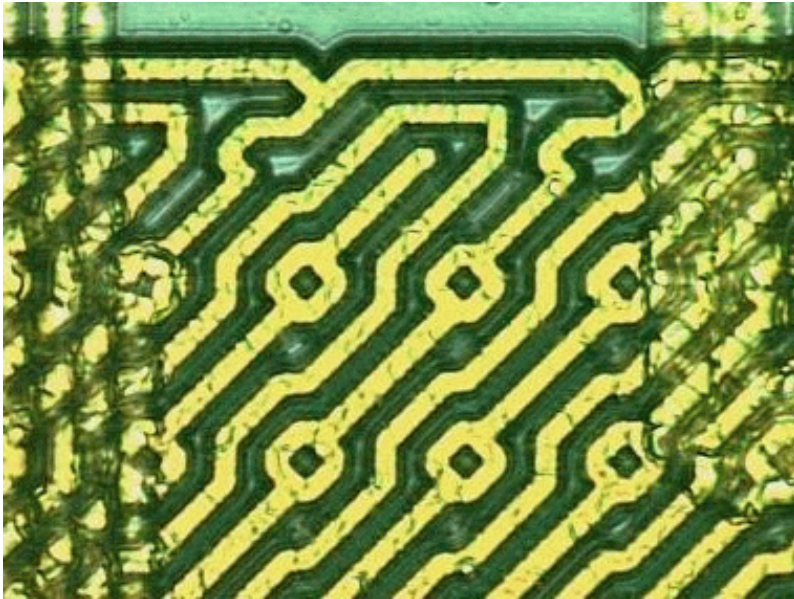
Test circuitry can be located on the 80-200 μm wide area between the dies that is removed during wafer cutting.



Blown polysilicon fuse near test pad (Motorola)

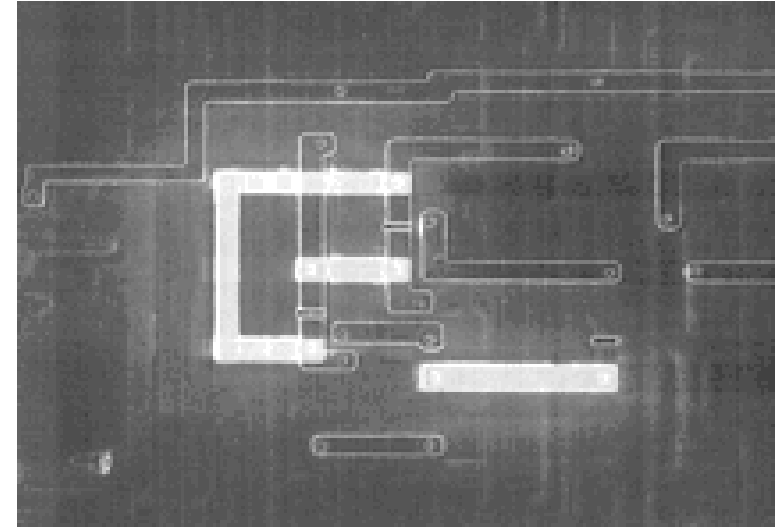


Example of a Top-Layer Sensor Mesh

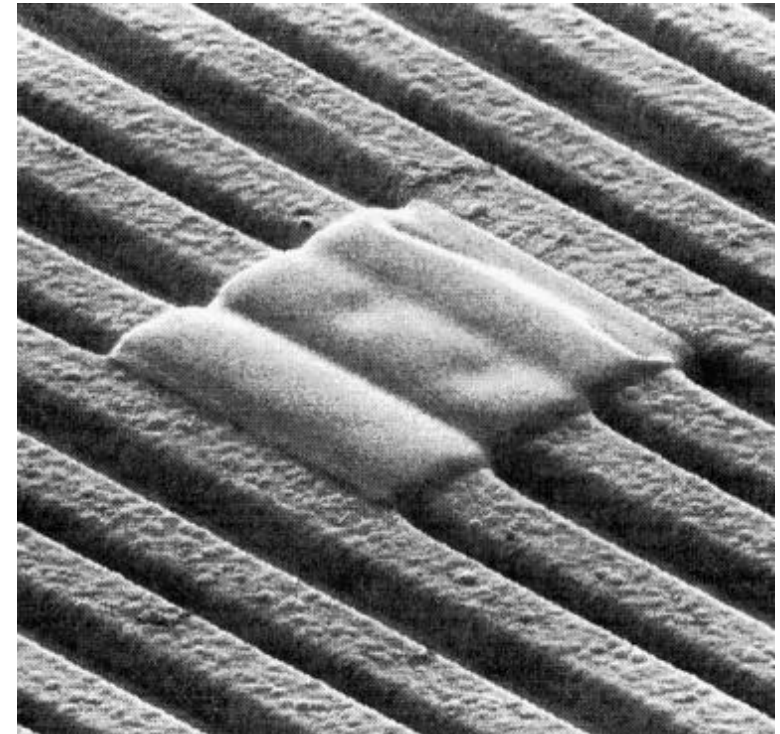


The sensor line is checked during operation for interruptions or short-circuits, which trigger alarms (e.g., processor halt or flash erase). The power lines are at some places used to supply the circuits below.

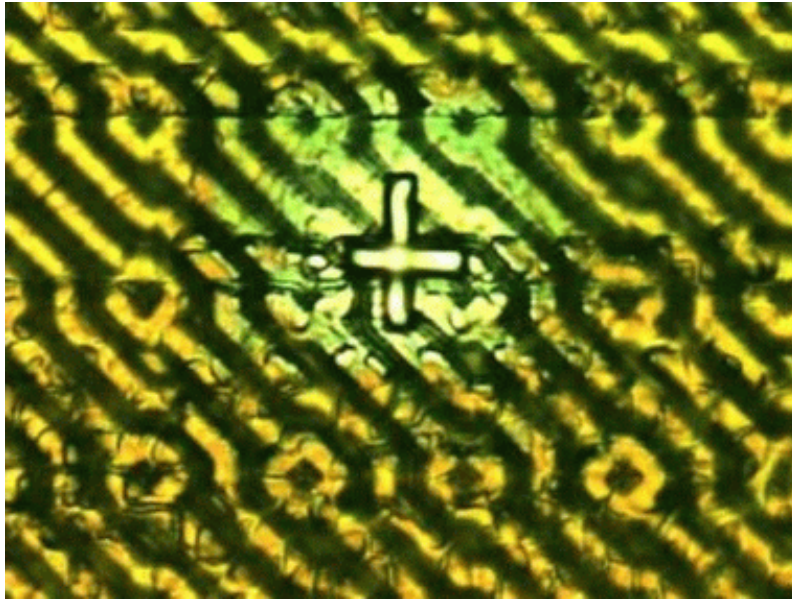
Focused Ion Beam Workstations for IC Modification



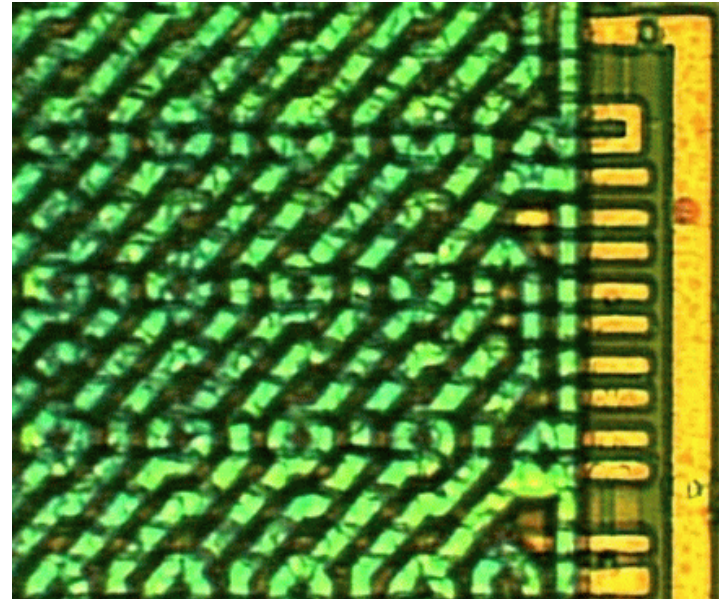
Focused ion-beam machines make high-resolution images of chip structures and allow us to both remove and deposit materials (metal and insulators) with $0.01\text{ }\mu\text{m}$ resolution. Gallium ions are accelerated with 30 kV and process gases like iodine or an organo-metallic compound are injected near the target location.



Sensor Meshes: Vulnerabilities and Attacks

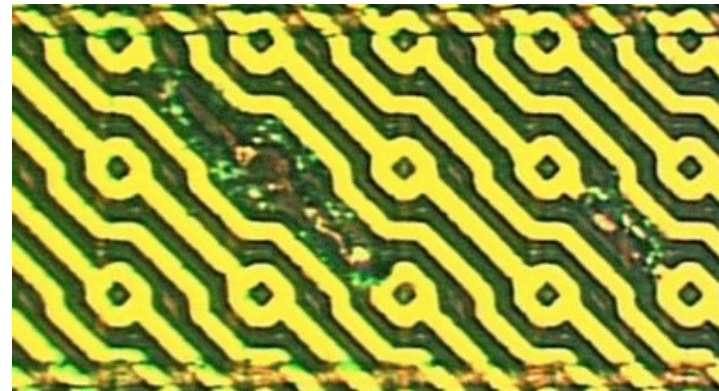


a)



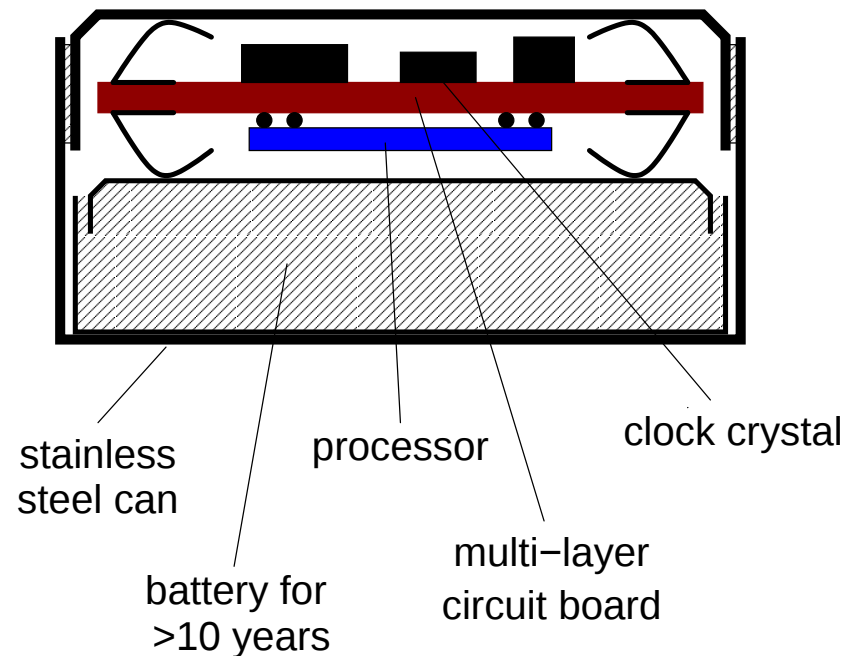
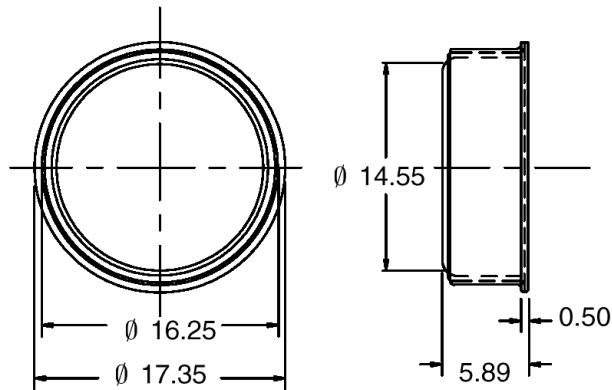
b)

- a) FIB workstation can be used to place a new via between mesh lines with an access cross on top for easy microprobing.
- b) Design flaw: redundant bus lines extend beyond the sensor mesh, allowing easy microprobing access ("Freedom for imprisoned crypto bits!").
- c) Not all power supply lines are used, so they can be removed with a laser cutter to allow access to signals below the mesh.



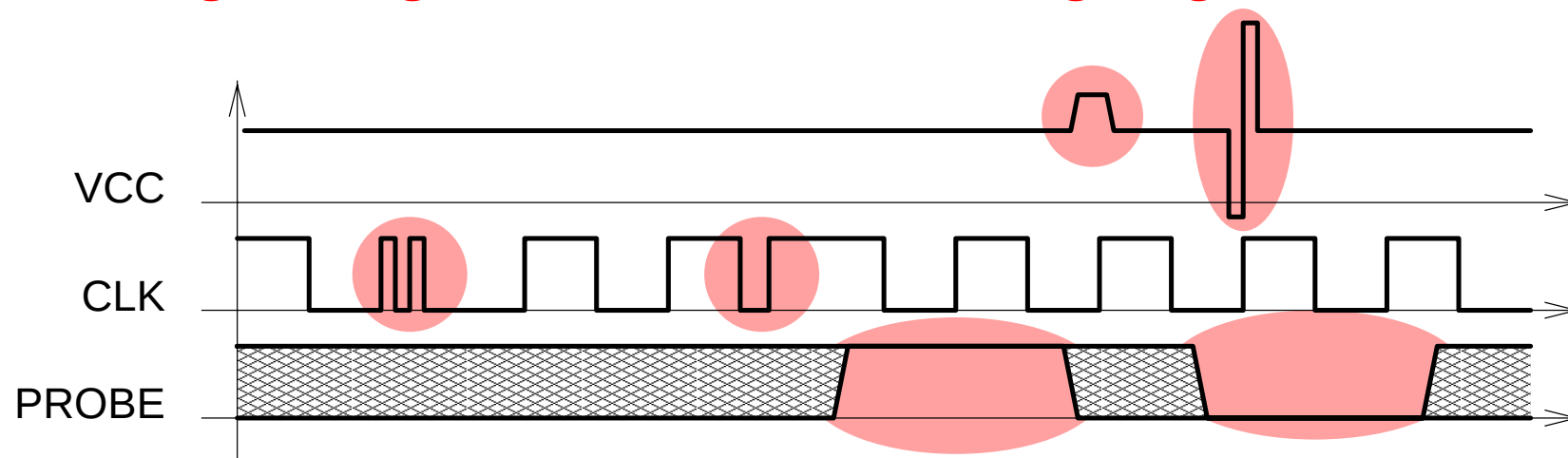
c)

iButtons – An Alternative Tamper-Resistant Module Form

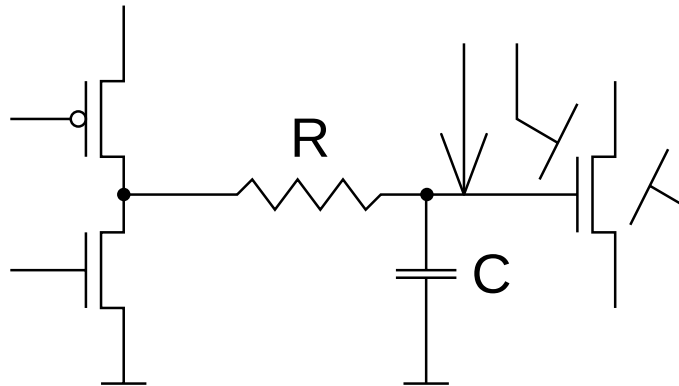


- battery-buffered on-chip SRAM
- sealed steel can provides mechanical stability and EMI shielding, which allows very sensitive alarm mechanisms
- multiple layers of sensor wires on chip and in circuit board
- chip layout facing circuit board
- difficult to open can without interrupting battery voltage
- pressurized with nitrogen

Change Single Instructions Using Signal Glitches



Fault model:



- Links between gates form RC delay elements
- R and C vary between links and individual chips
- Max. RC sum of any signal path determines max.CLK frequency
- External electrical fields could open/close channels
- Transistors compare V_{CC} and V_C , which allows VCC glitches

Glitch attack on an output loop

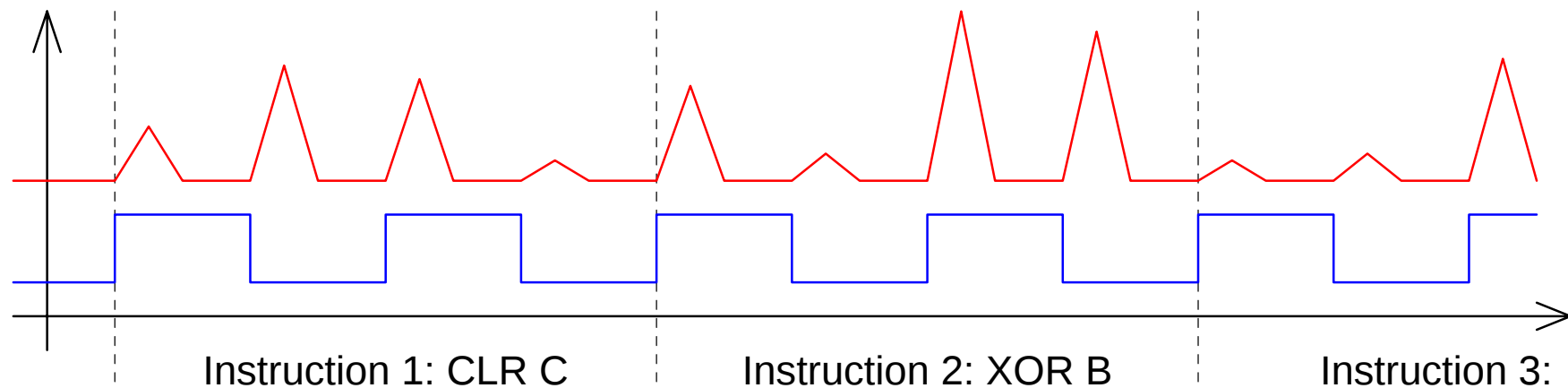
Typical data output routine in security software:

```
1  b = answer_address
2  a = answer_length
3  if (a == 0) goto 8
4  transmit(*b)
5  b = b + 1
6  a = a - 1
7  goto 3
8  ...
```

Cause CLK or VCC glitch when instruction 3 or 6 is being fetched, in order to extend loop length to send additional memory content to port.

Power Supply Current Forms a Significant Covert Channel

Record current in VCC/GND connection with 12-bit, 30-MHz ADC, in order to reconstruct executed instruction sequence and observe cryptographic computations.



- Characteristic current spikes can identify executed instruction
- Data values appear in power profiles either as differential Hamming weights (~0.5-1 mA/bit) or as individual bits, e.g. with multiplication or shift instructions
- Current signature depends on accessed memory type (SRAM-write short circuit, EEPROM read-out amplifier, etc.)
- Activation of EEPROM programming-voltage charge pump observable, which allows to abort before state changes (e.g., with bad retry counters)

Tamper Resistance versus Tamper Evidence

Invasive attacks

- Microprobing
 - FIB editing
 - Layout reconstruction
- violate tamper resistance requirement
(FIPS 140-1 Level 4)

Require between hours and weeks in a specialized laboratory, therefore the owner of the card is likely to notice the attack and can revoke certificates for keys that might be lost.

Non-invasive attacks

- Glitch attacks
 - Power analysis
 - Software vulnerabilities
- violate in addition tamper-evidence requirement
(FIPS 140-1 Level 2)

Can be performed within a few seconds inside a Trojan terminal in a Mafia-owned shop, therefore card owner will not notice that card secrets have been stolen and will not revoke keys.

Classification of Attackers

- Class I: Clever Outsiders.** Often very intelligent, have insufficient knowledge of the system, have access to moderately sophisticated equipment, use existing weaknesses in the system.
- Class II: Knowledgeable Insiders.** Substantial specialized technical education and experience, varying degrees of understanding of the system but potential access to most relevant information, often highly sophisticated tools.
- Class III: Funded Organizations.** Teams of specialists with complementary skills, great funding resources, capable of in-depth analysis and design of sophisticated attacks, most advanced tools, access to knowledgeable insiders.

[according to Abraham, Dolan, Double, Stevens: Transaction Security System, IBM Systems Journal, Vol. 30, No. 2, 1991.]