

Design Principles for Tamper-Resistant Smartcard Processors

Oliver Kömmerling

ADSR



Markus G. Kuhn

Computer Laboratory



**UNIVERSITY OF
CAMBRIDGE**

[http://www.cl.cam.ac.uk/~mgk25/sc99-tamper\[-slides\].pdf](http://www.cl.cam.ac.uk/~mgk25/sc99-tamper[-slides].pdf)

Classes of Attacks on Security Modules

Microprobing

Open the package, access the chip surface with semiconductor test equipment, and observe and manipulate the internal data paths

Software Attacks

Use the normal communication interface and abuse security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation

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 timings

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.

Tamper Resistance versus Tamper Evidence

Invasive attacks

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

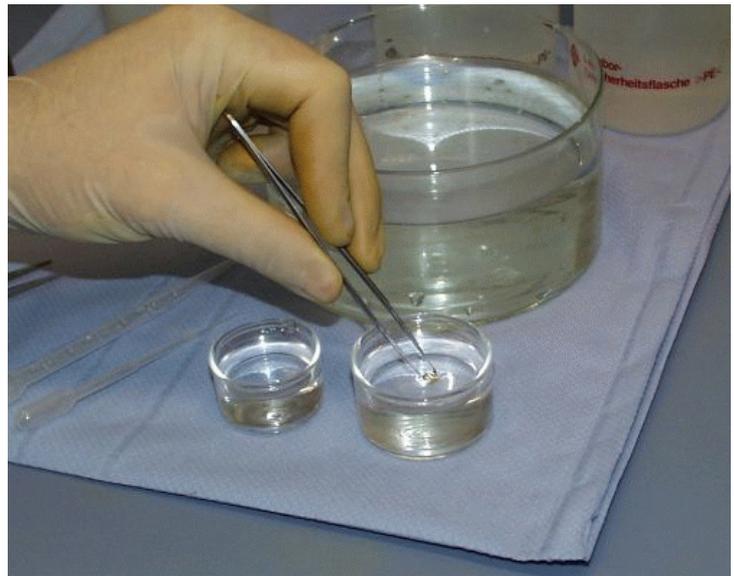
Require between hours and weeks in a specialized laboratory, therefore the owner of the card is likely to notice the attack and can revoke certificates for keys that might be lost.

Non-invasive attacks

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

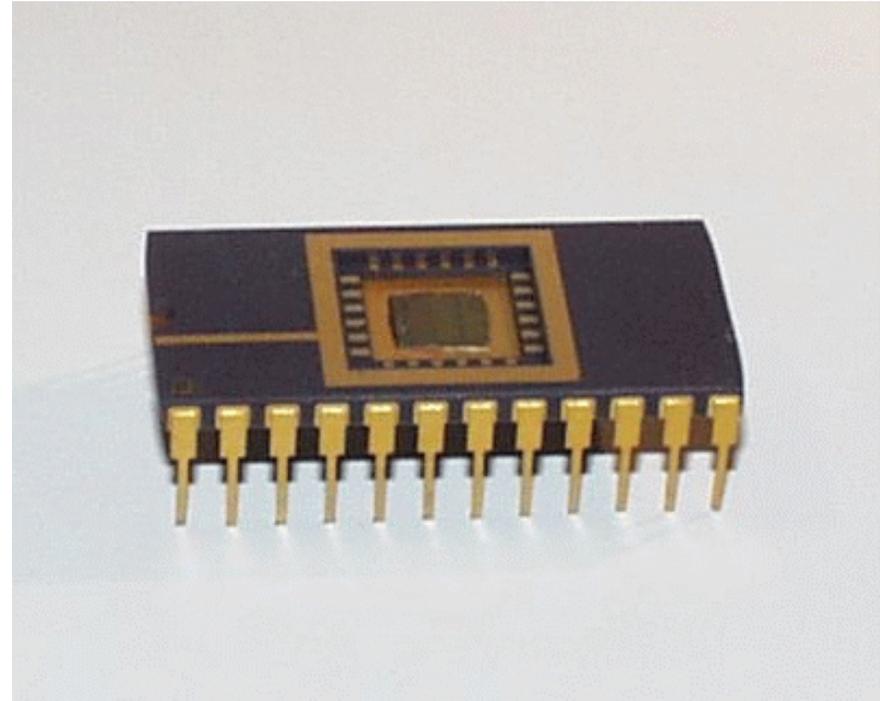
Can be performed within a few seconds inside a Trojan terminal in a Mafia-owned shop, therefore card owner will not notice that card secrets have been stolen and will not revoke keys.

Preparation I: Depackaging the Processor



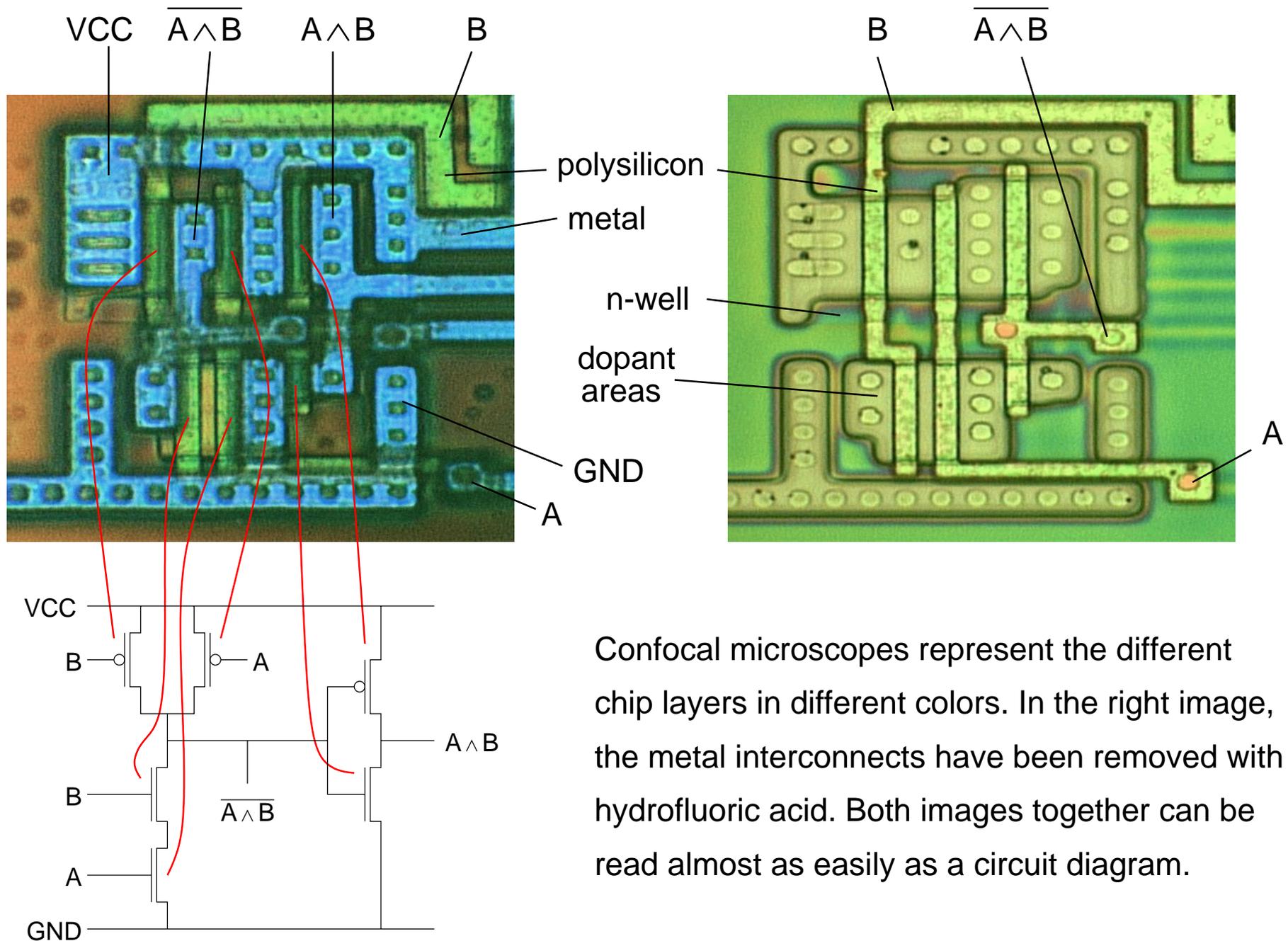
- 1) Heat up card plastic, bend it, and remove chip module
- 2) Dissolve package in 60 °C fuming nitric acid, then wash in acetone, deionized water, and finally isopropanol. The etching should be carried out under very dry conditions.

Preparation II: Bonding into a Test Package



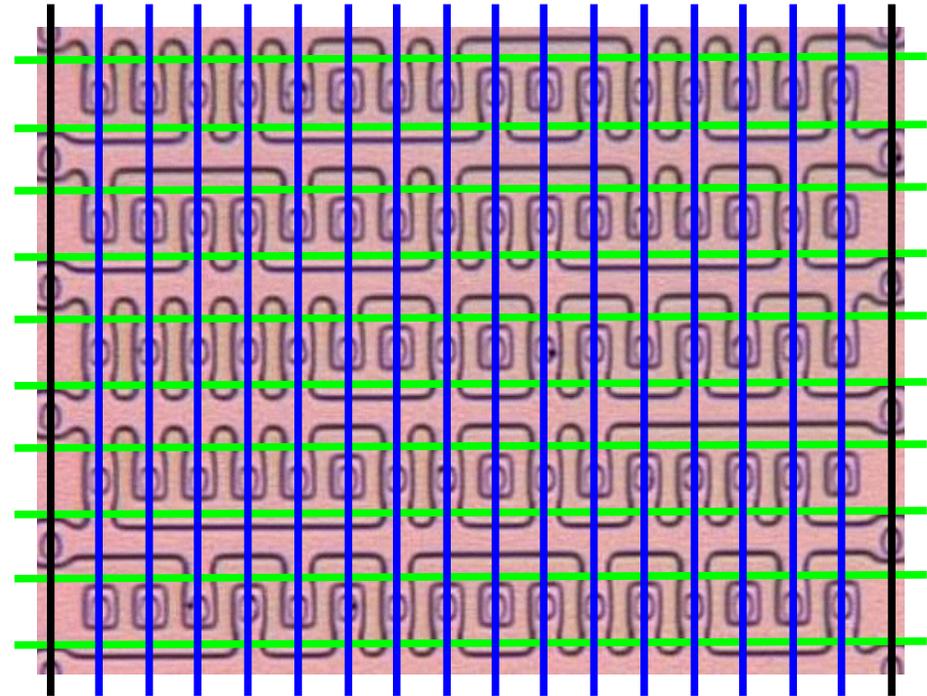
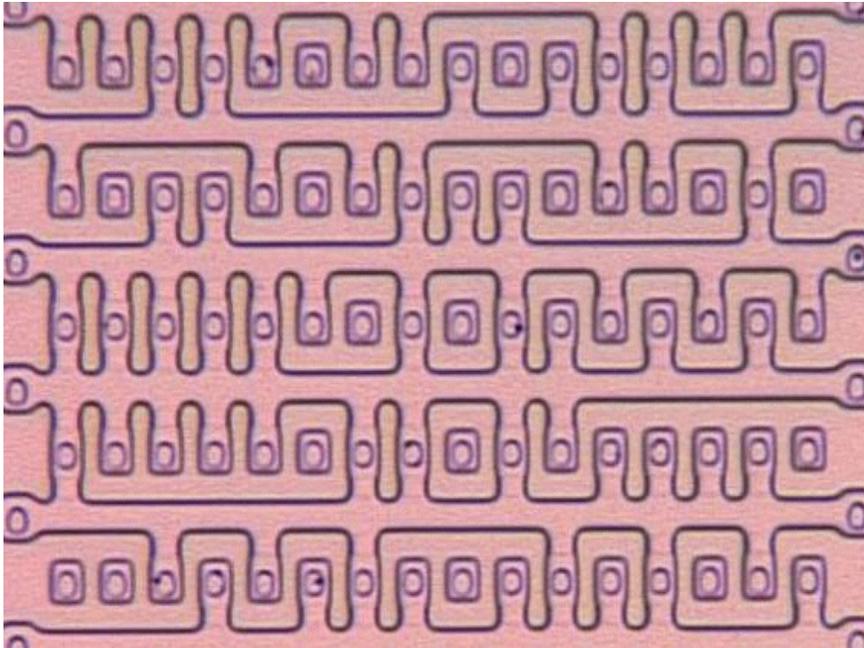
A manual bonding station establishes reliable contacts to the supply, communication, and test pads of the microprocessor using ultrasonic welding of a fine aluminium wire.

Optical Reverse-Engineering of VLSI Circuits



Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

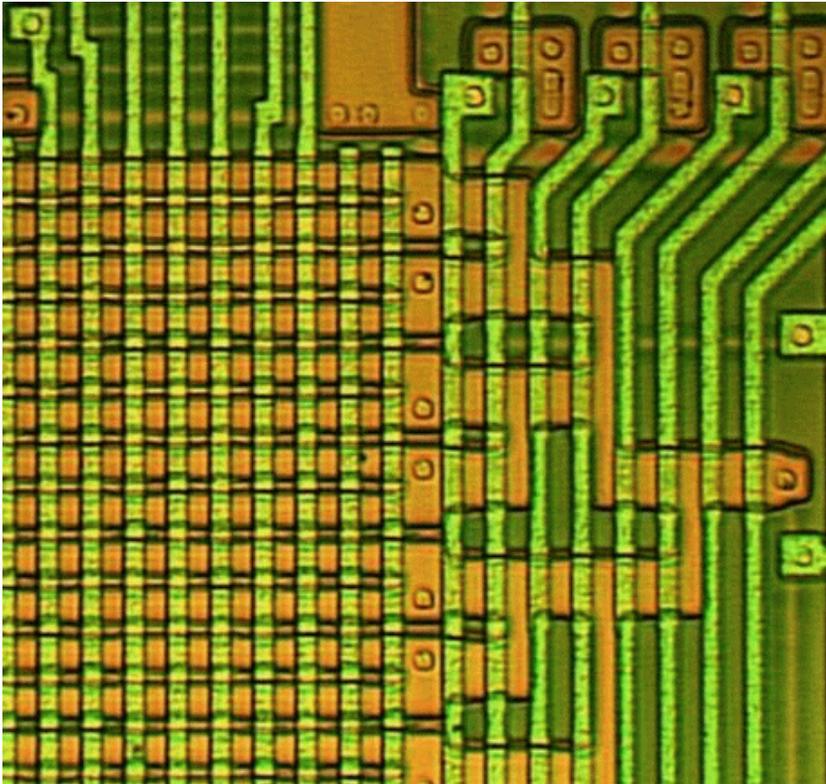
Optical Access to Diffusion Layer ROM Content



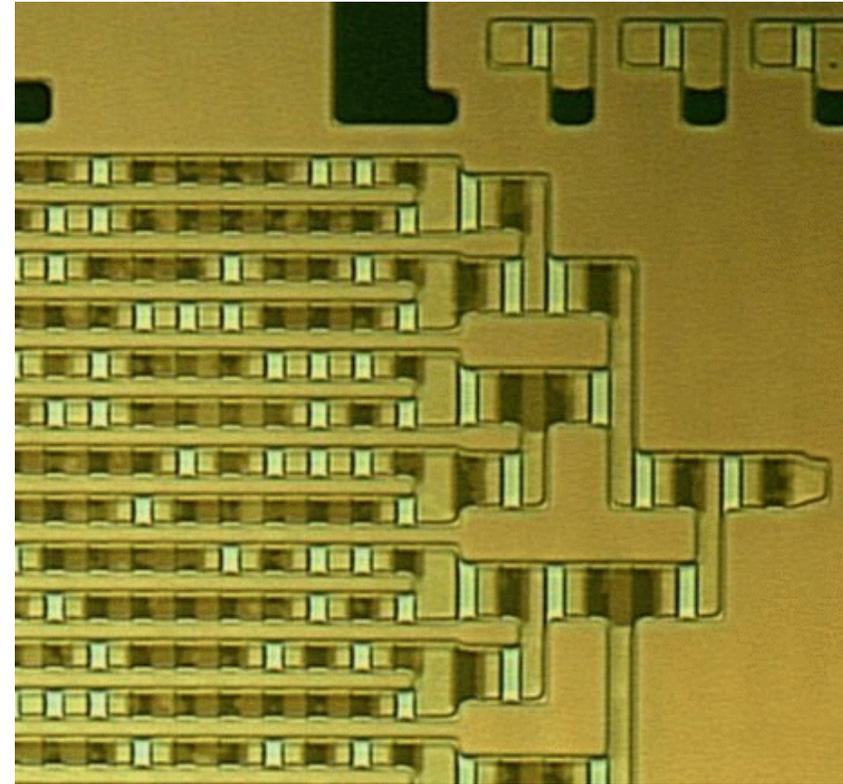
After all covering layers including the surrounding field oxide have been removed with hydrofluoric acid, the shape of the now visible diffusion areas will reveal the ROM content (here 16x10 bits).

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

Optical Reconstruction of Ion Implantation ROM Content



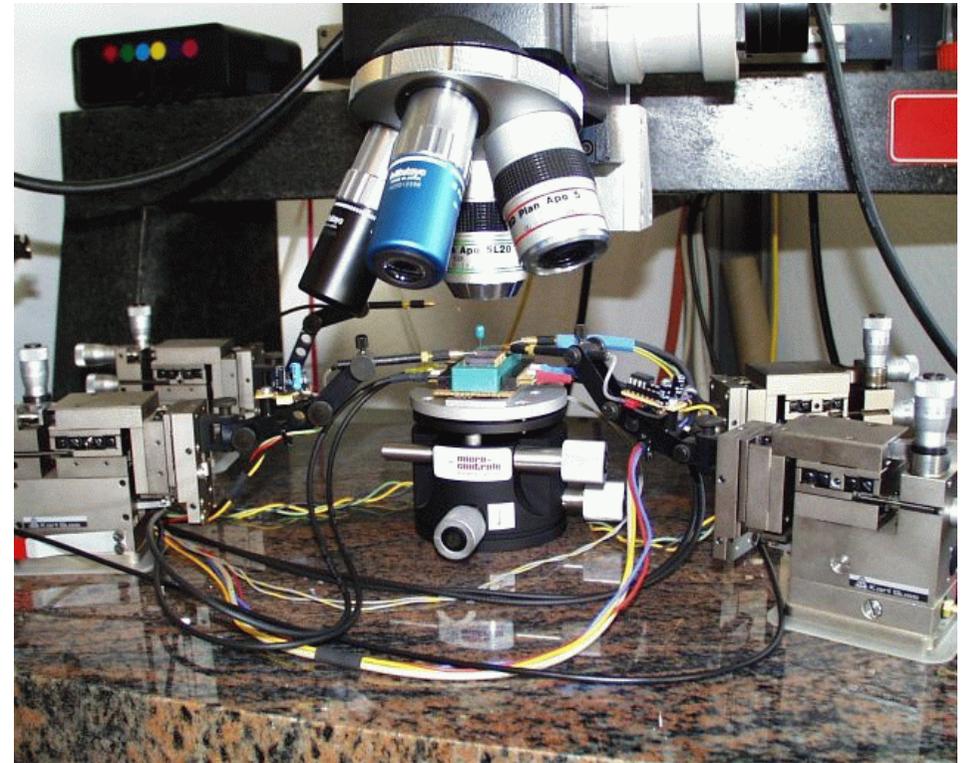
View of ROM with polysilicon intact



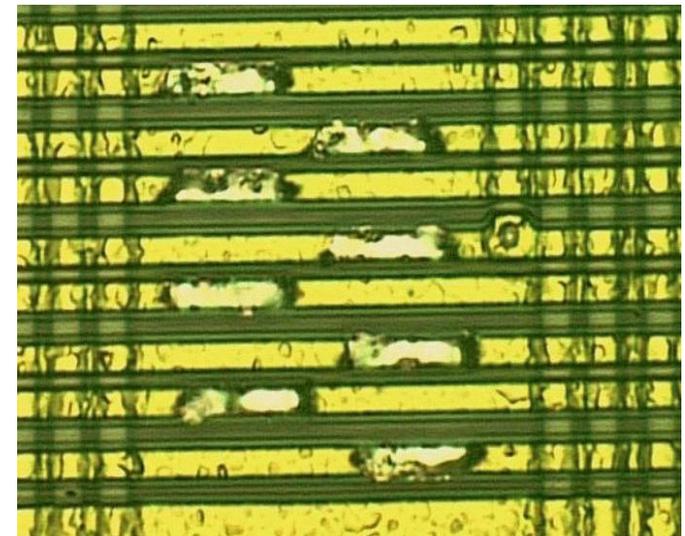
Diffusion layer after crystallographic etch

This type of ROM does not reveal the bit pattern in the shape of the diffusion areas, but a crystallographic staining technique (Dash etch) that etches doped regions faster than undoped regions will still show the ROM bits.

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.



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:

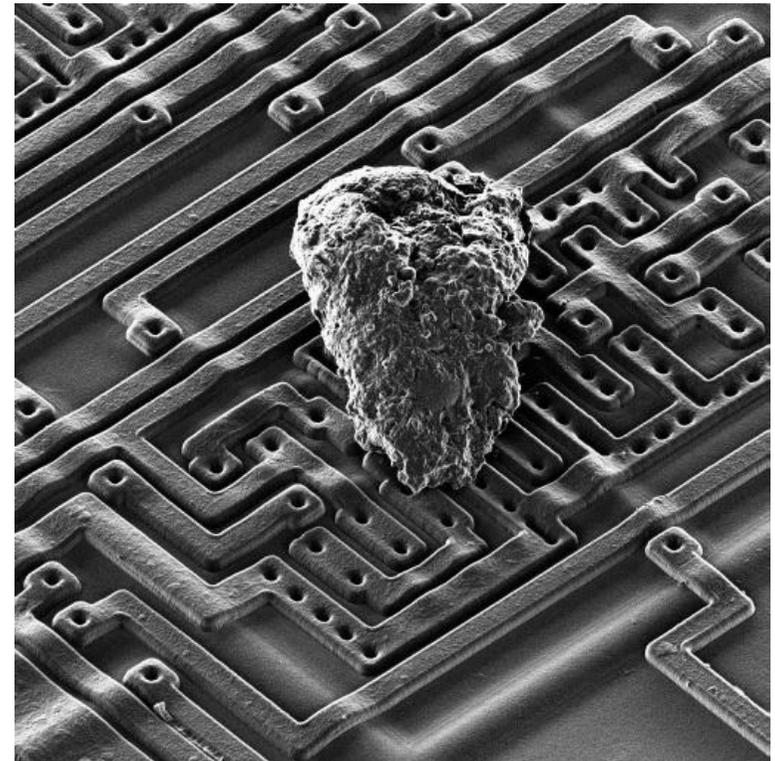
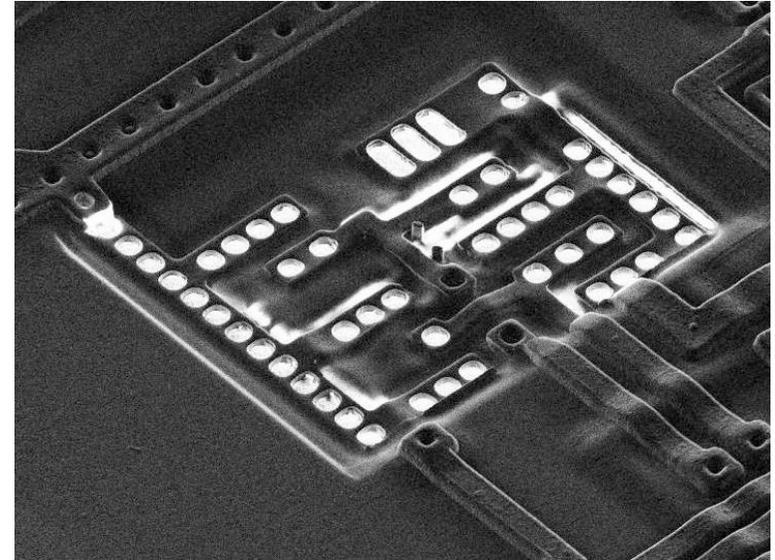
Abuse existing processor hardware as an address generator that accesses all memory locations predictably. A single probing needle can now capture all memory values, probing one bus line at a time.

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!

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 $0.01 \mu\text{m}$ resolution. Gallium ions are accelerated with 30 kV and process gases like iodine or an organic compound are injected near the target location.

Electron Beam Testing

Modified scanning electron microscope (SEM) with voltage contrast function.

Primary electrons (2.5 kV, 5 nA) hit secondary electrons out of the target location.

Number and energy of secondary electrons recorded by spectrometer and detector indicates local field potential.

This allows contact-free signal measurements on the chip.

Limitation:

Measured signal is the low-pass filtered product of the beam current multiplied with a function of the signal voltage.

- Stroboscopic measurements allow to capture periodic signals with a bandwidth of several gigahertz
- Real-time voltage contrast observation of a non-periodic signal is limited to a few megahertz

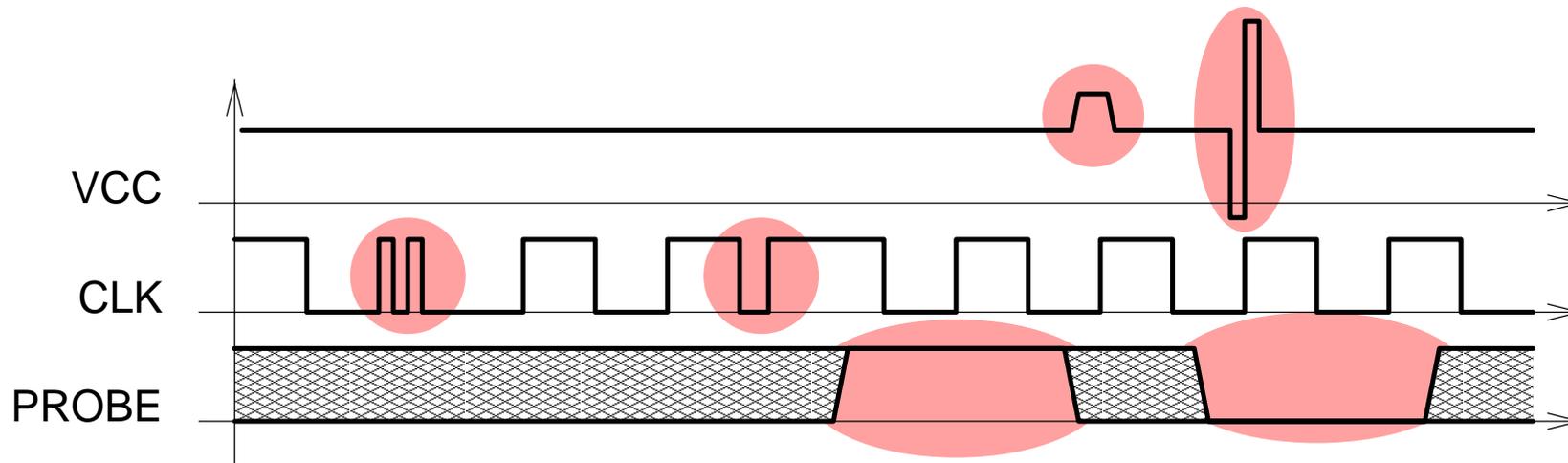
Analog Circuit Characteristics Allow Non-Invasive Attacks

- Delays vary along various signal paths (RC and gate count)
- Flip-flops sample input during a short interval and compare it with the supply voltage levels.
- Flip-flop metastability
- Brief short-circuit when CMOS gate changes state
- Significant short-circuit when SRAM cell changes state
- Capacitive loads draw current when a gate changes state
- Static current consumption extremely small
- ... plus many other physical and electronic effects ...

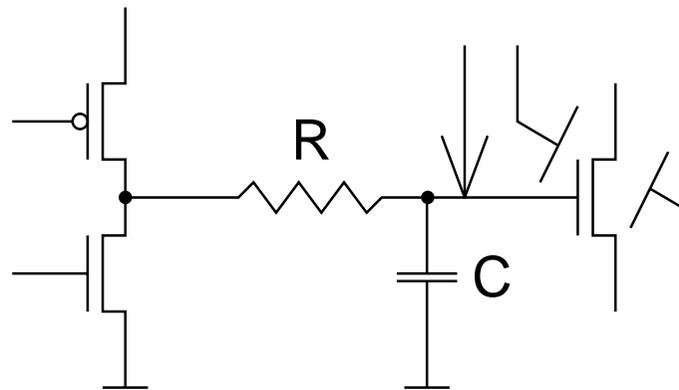
Smartcards are particularly vulnerable to non-invasive attacks because the attacker has full control over power and clock supply lines and environmental conditions.

Careful security reviews must usually include detailed analog VLSI simulations. Smartcard security cannot be achieved by studying only a digital abstraction of the processor design.

Change Single Instructions Using Signal Glitches



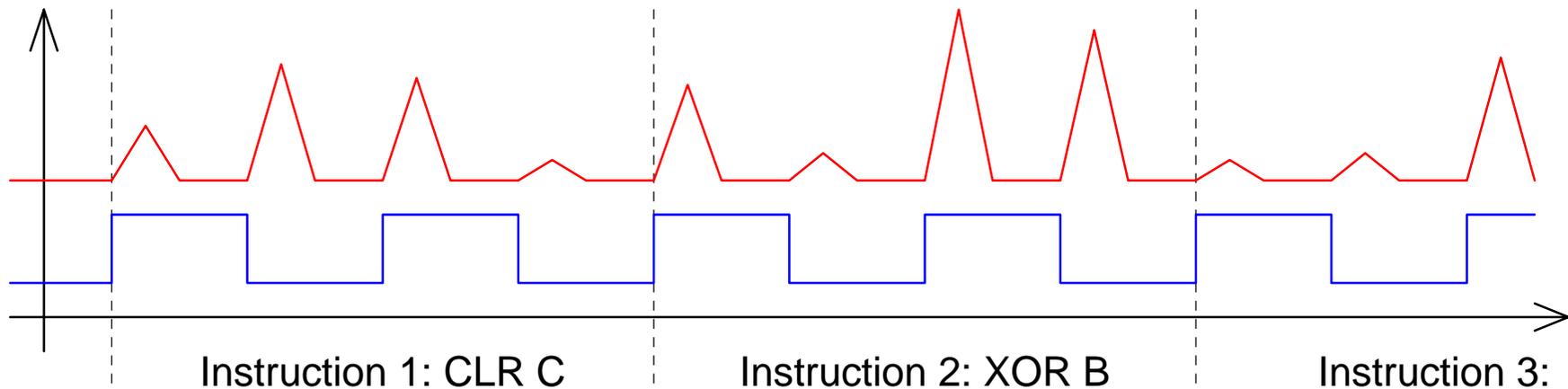
Fault model:



- 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

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)

Non-Deterministic Processors Complicate Observation

Randomized Internal Clock Signal

- Hardware random-bit generator supplies internal clock signal. After 1000 external clock cycles, 200-300 internal clock cycles have been executed internally (binomial distribution).
- Only timer and I/O shift registers are directly operated by external clock.
- Dummy loads are activated during rest periods to suppress the random sequence in the supply current.

Randomized Instruction-Level Multithreading

- Every register and latch (except SRAM) is replicated, including stack pointer, program counter, and instruction register.
- Hardware random-bit generator schedules per instruction cycle between the two or more threads of execution that run on these register sets.
- Parallel encryption or background dummy operations introduce non-determinism and correlated covert-channel noise.

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:

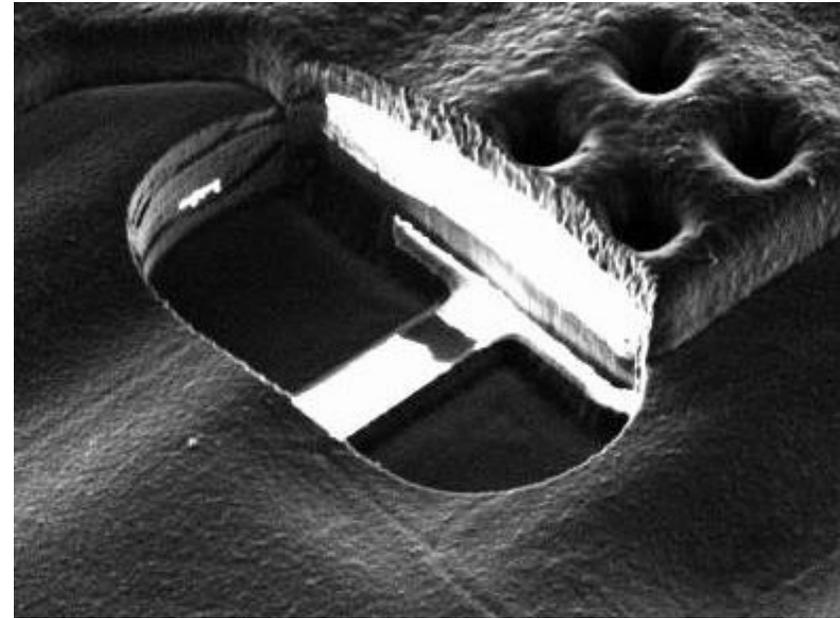
- Parallel/serial converters for full bus
- Full bus available on large probing pads

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

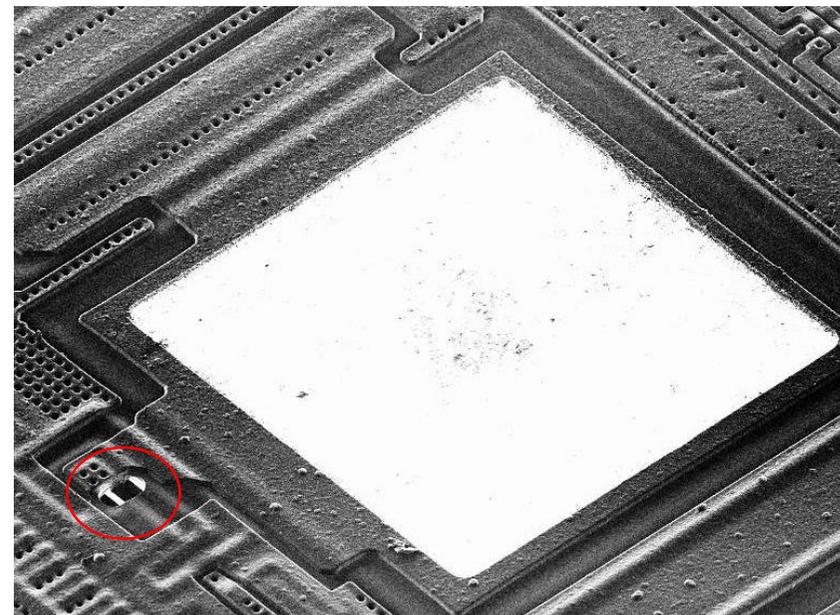
Solution:

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)



Restricted Program Counter

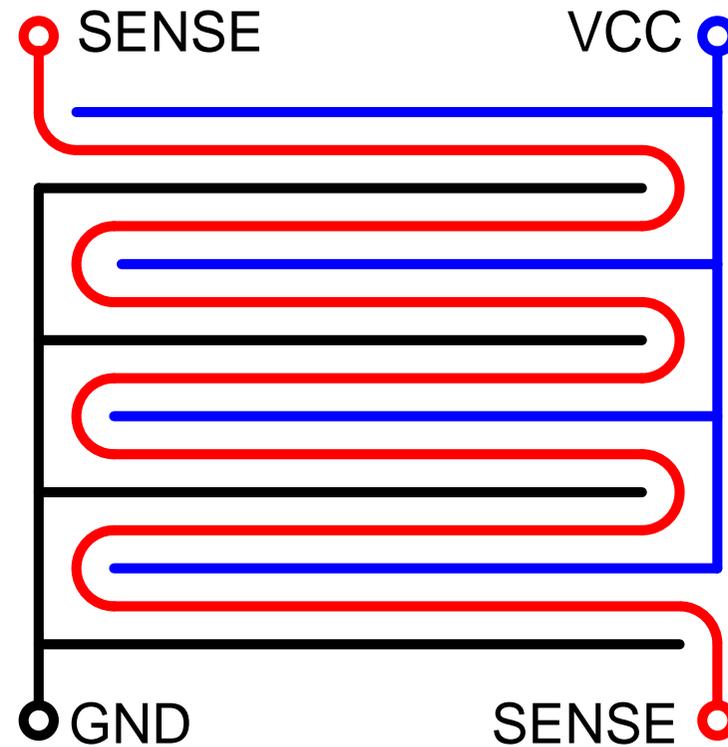
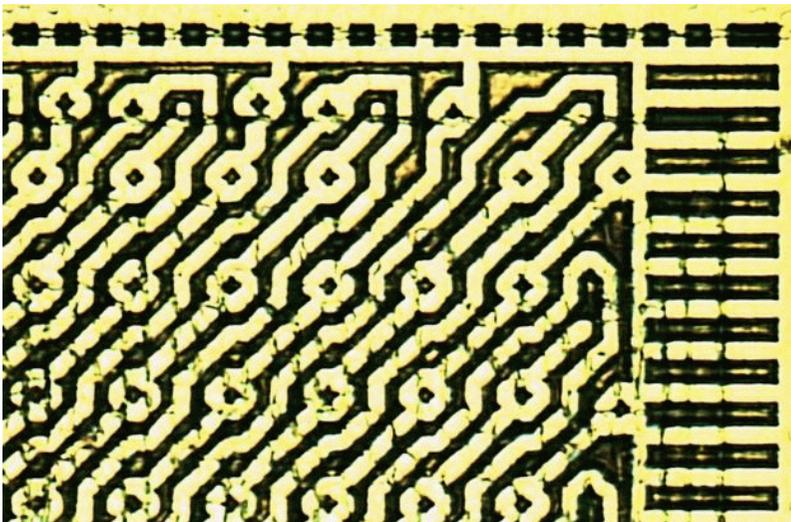
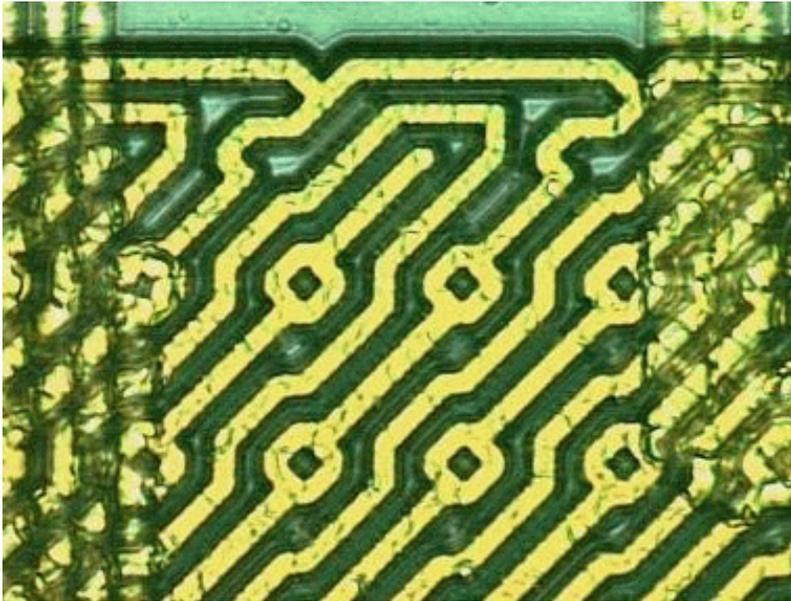
A standard program-counter mechanism is too easily abused as an address-sequence generator. Tamper-resistant design of the instruction decoder is difficult. Watchdog circuitry requires many transistors and simple forms are also easily disabled.

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.

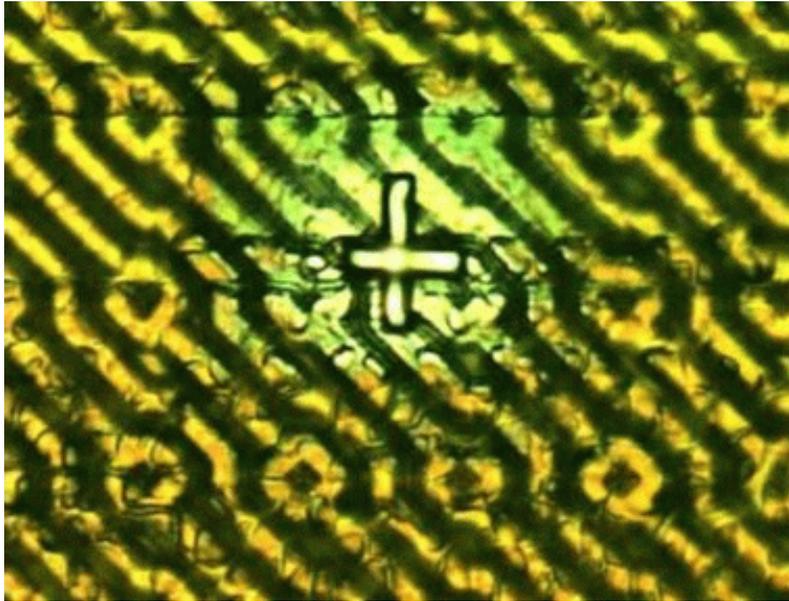
Now, no simple FIB edit can cause the program counter to cover all addresses.

Example of a Top-Layer Sensor Mesh

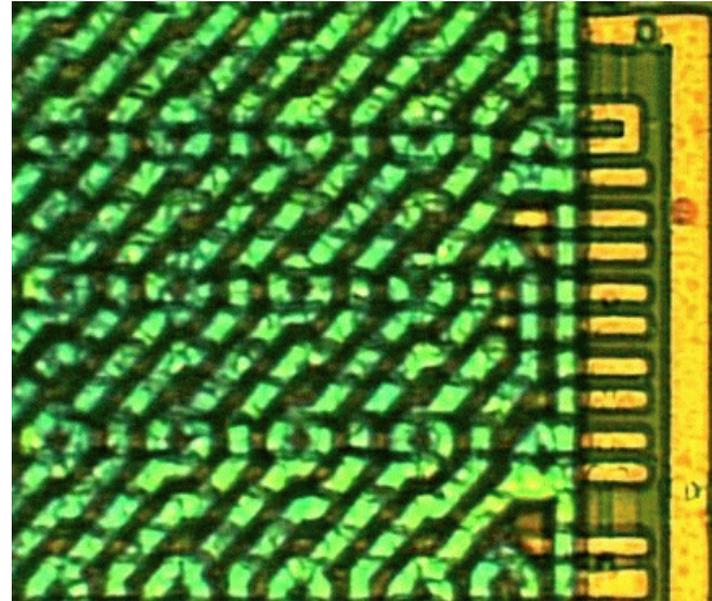


The sensor line is checked during operation for interruptions or short-circuits, which trigger alarms (e.g., processor halt or flash erase). The power lines are at some places used to supply the circuits below.

Sensor Meshes: Vulnerabilities and Attacks



a)

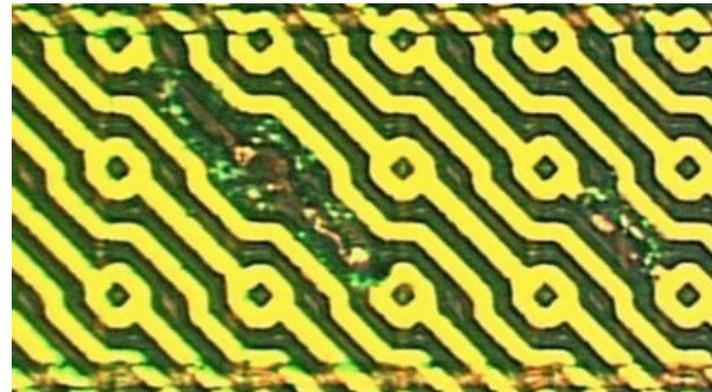


b)

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)

Summary and Conclusions

- Invasive techniques break all currently available smartcards and have led to continued conditional-access smartcard piracy since 1994
- Non-invasive attacks (glitching, current analysis) are the main concern only in tamper-evidence applications (banking, signatures), because microprobing is generally the far easier and more universal type of attack
- Examples for lowest-cost countermeasures that are not yet implemented widely or in effective ways:
 - randomized clock
 - instruction multi-threading
 - constant-current regulators
 - destruction of test circuits
 - tamper-resistant sensors
 - top-layer sensor mesh
 - loosely coupled clock PLL
- Smartcard form probably unsuitable for strong tamper-resistance requirements (conditional access, copy protection), better use battery-backed SRAM
- Extremely careful engineering might lead to high tamper-evidence assurance for smartcards one day (for banking, authentication, digital signatures)