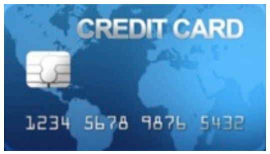
Low-Cost Chip Microprobing

Philipp Maier <dexter@srlabs.de>
Karsten Nohl <nohl@srlabs.de>

SECURITY RESEARCH LABS

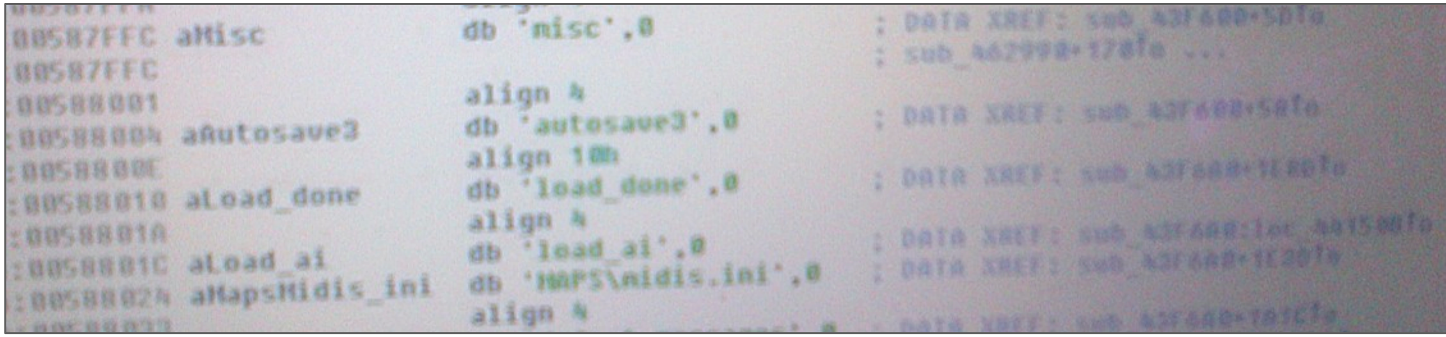
A few smart cards chips cover numerous security domains

	Security chip applications
	Payment cards, electronic ID cards, access badges
	Trusted platform modules (TPM)
	Device and accessory identification
	SIM cards, NFC secure elements
	Content protection

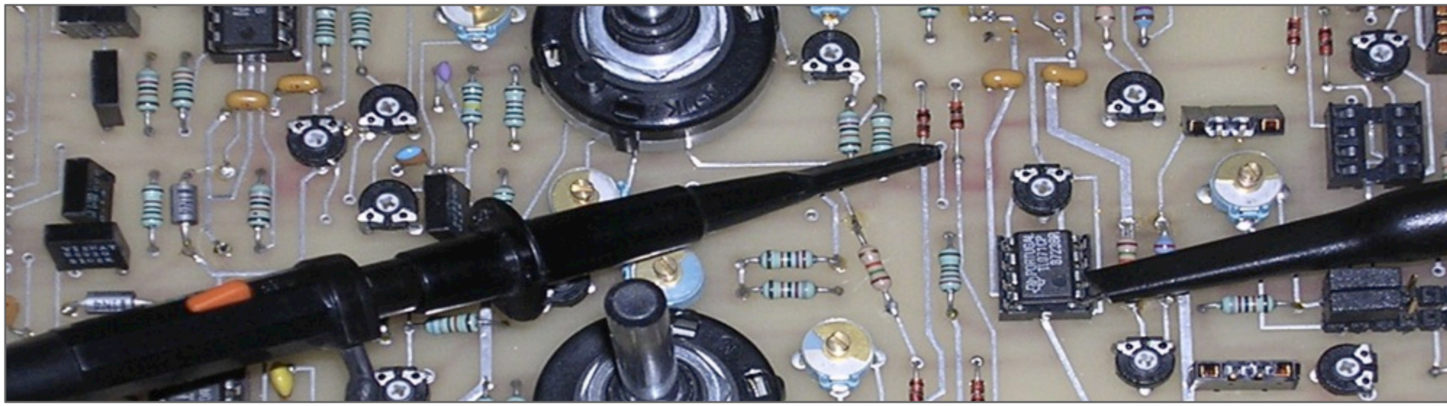
Chip hacking motivation

- Recent trend – Functionality that users traditionally circumvented or exposed in their devices moves into hardware:
  - Usage restrictions
  - DRM, “Dongeling”
  - “Secret” protocols
- Devices are increasingly controlled by their manufac-turer, not their owner
- We need more wide-spread hardware analysis knowledge and cheaper tools to combat this trend

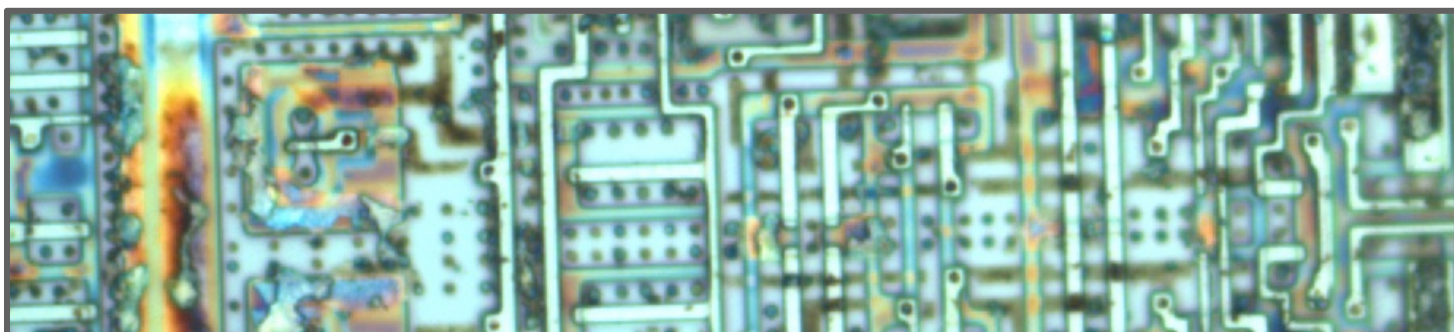
Reverse-engineering hardware functions requires specific tools



Disassamler, decompiler



Oscilloscope, logic analyzer



Microscope, micropositioner (this talk's focus)

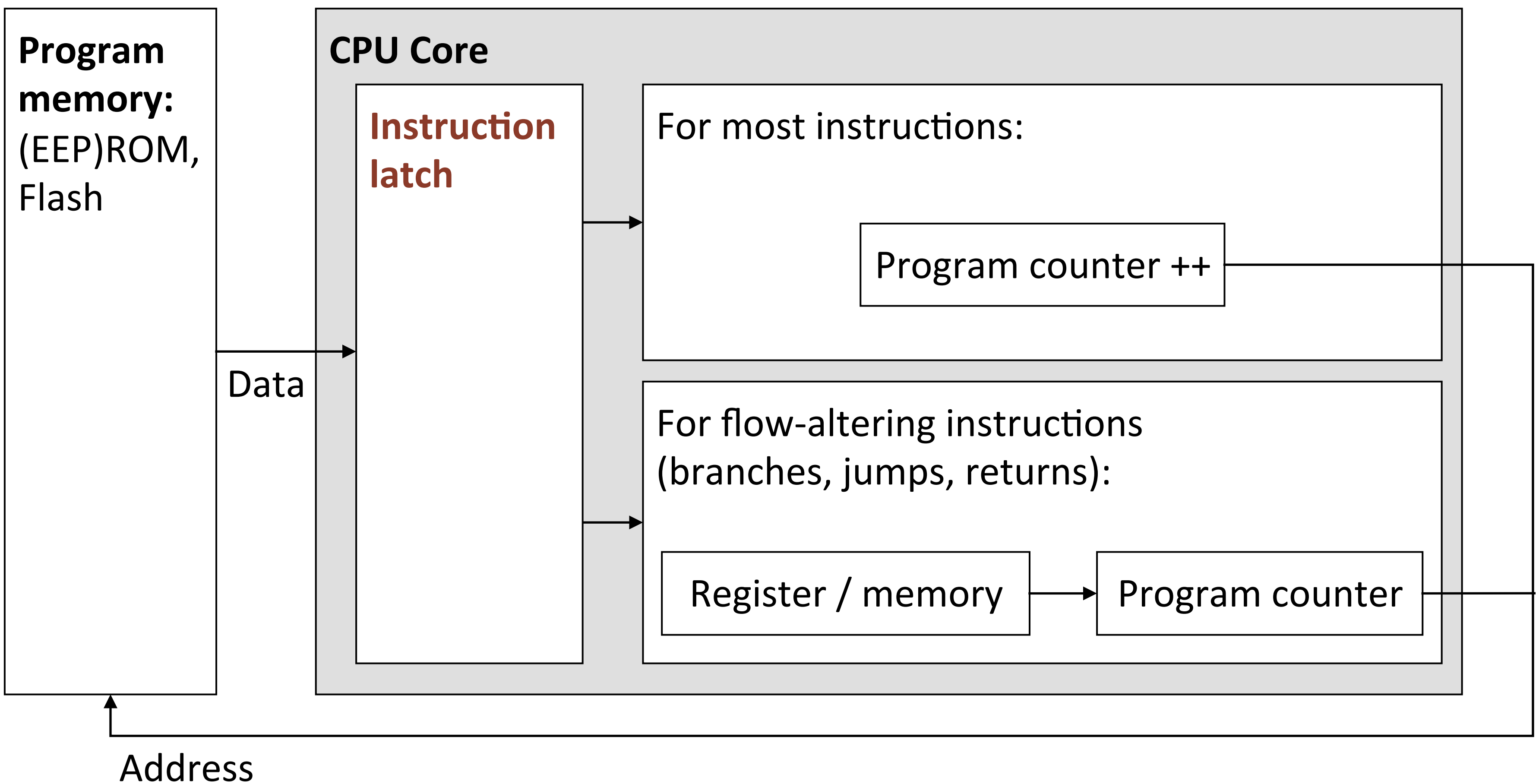
This talk introduces the methodology and tools of earlier (and hopefully future) works

	Reverse-engineer chip functionality	Read out memories
Introductory	**Deep Silicon Analysis** Starbug, Nohl **25C3, HAR 2009**	**This Talk** Dexter, Nohl **29C3**
	Reviving Smart Card Analysis Tarnovsky, Nohl **Camp 2011, BlackHat 2011**	
Advanced	**Mifare, Legic, DECT Reversing** Starbug, Plötz, deDECTed*, Nohl **24C3, 26C3**	**Hacking the Smart Card Chip** et al. Tarnovsky Various **BlackHat, ToorCon**

* deDECTed team: Karsten Nohl, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, Mathias Wenzel

- **Microprobing background**
- Probing with simple tools
- Advanced probing techniques

Basic CPU principle: Current instruction decides which instruction gets loaded next

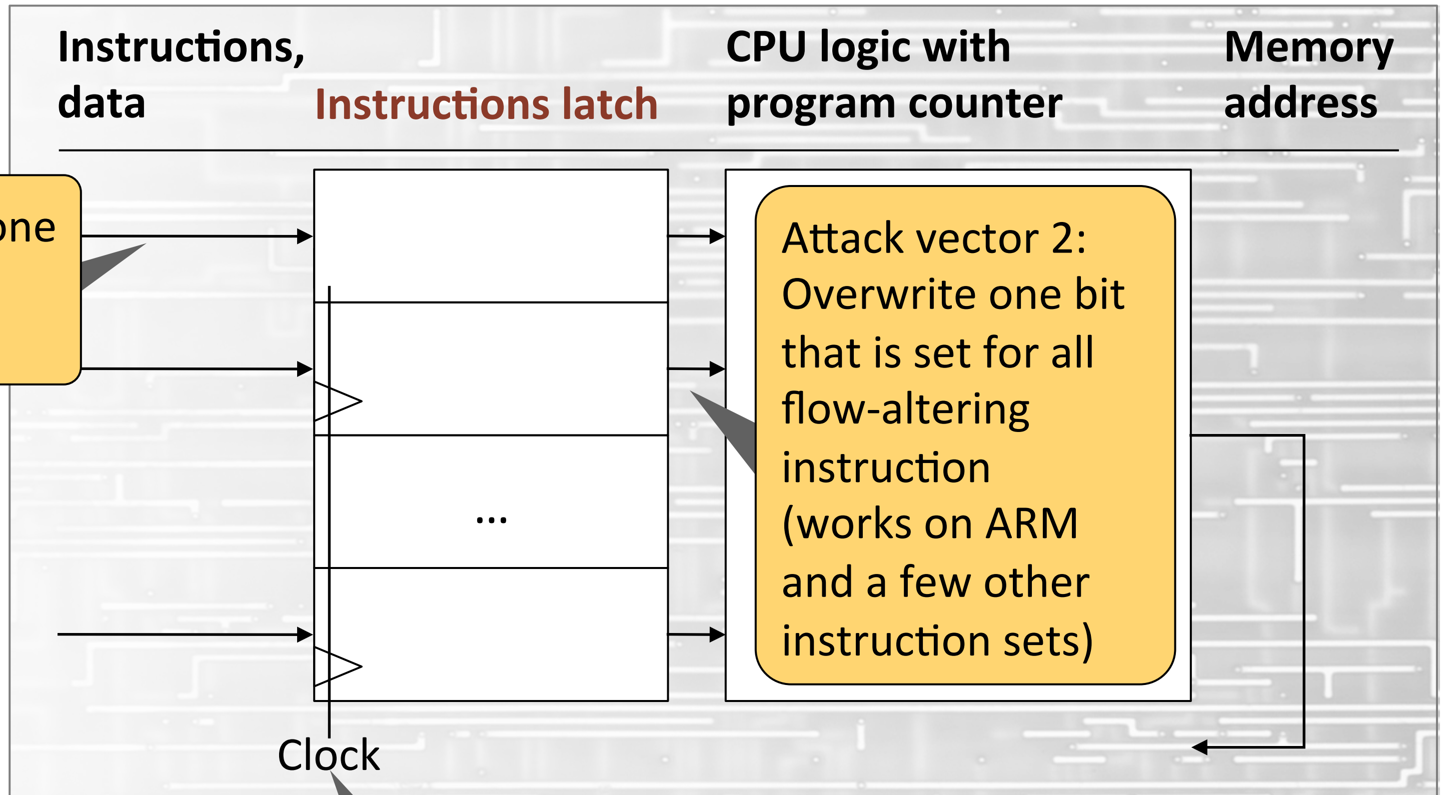


SECURITY RESEARCH LABS

Probing and glitching with only two needles allows full memory read-out

Attacker goal: Make the CPU go to all places in memory independent of security checks and other flow characteristics. This attack is called **Linear Code Extraction**.

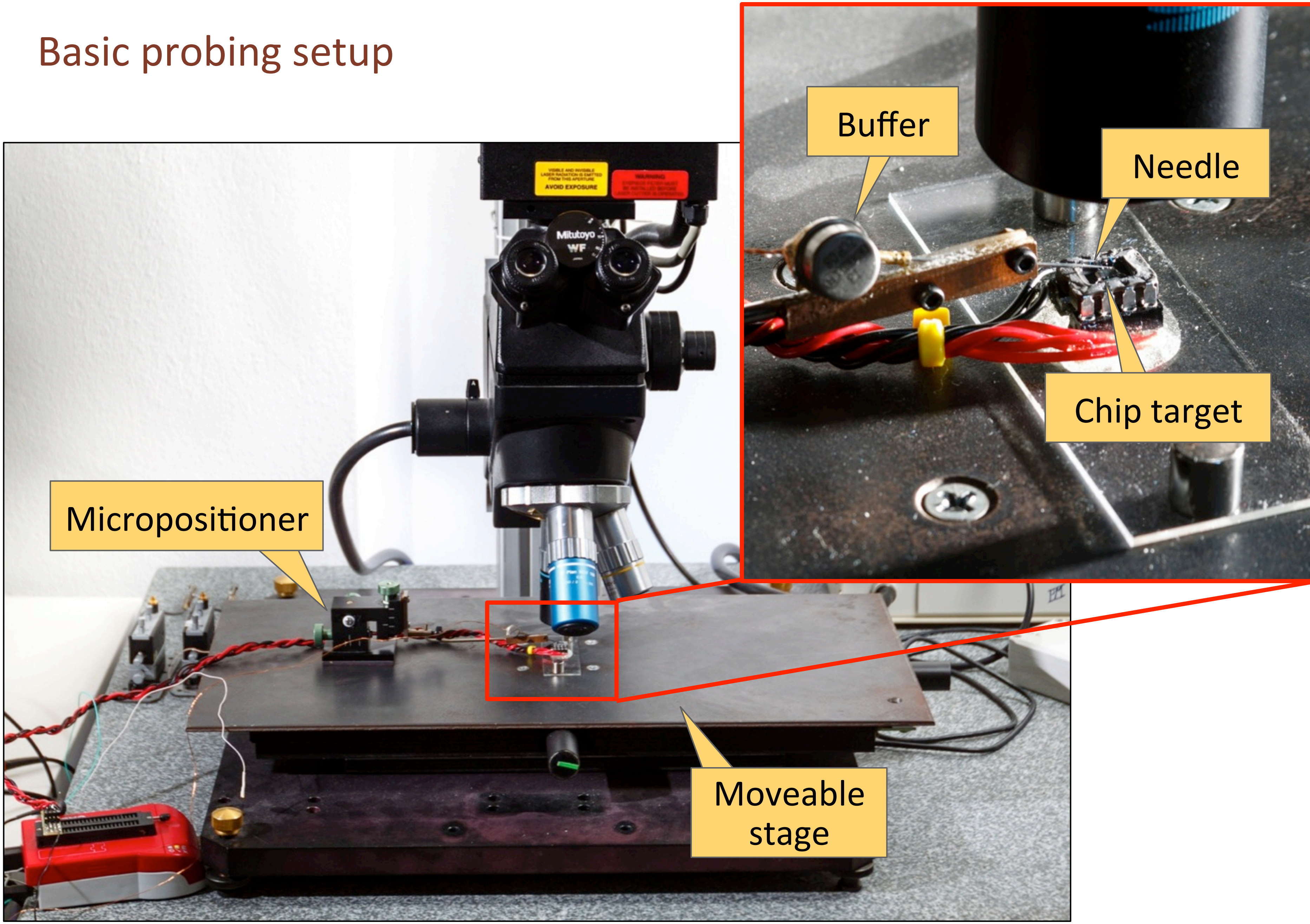
Attacker probes one bus bit at a time (first needle)



Attack vector 1: Freeze the latch clock so that one instruction is executed indefinitely (second needle)

- Microprobing background
- **Probing with simple tools**
- Advanced probing techniques

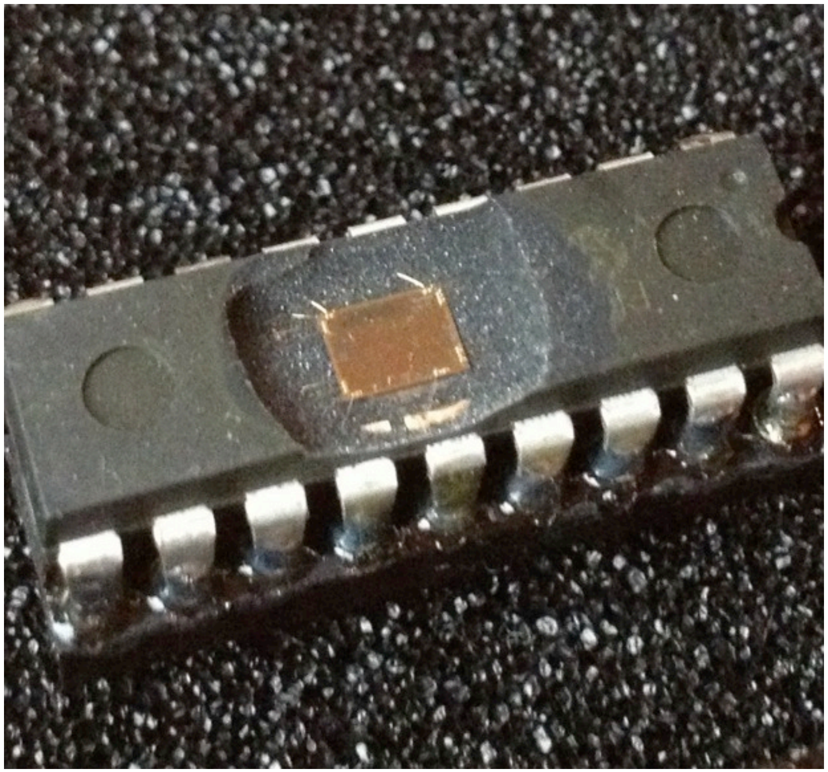
Basic probing setup



Step 1: Decapsulate chip

Option A – **Mechanically pry open package**

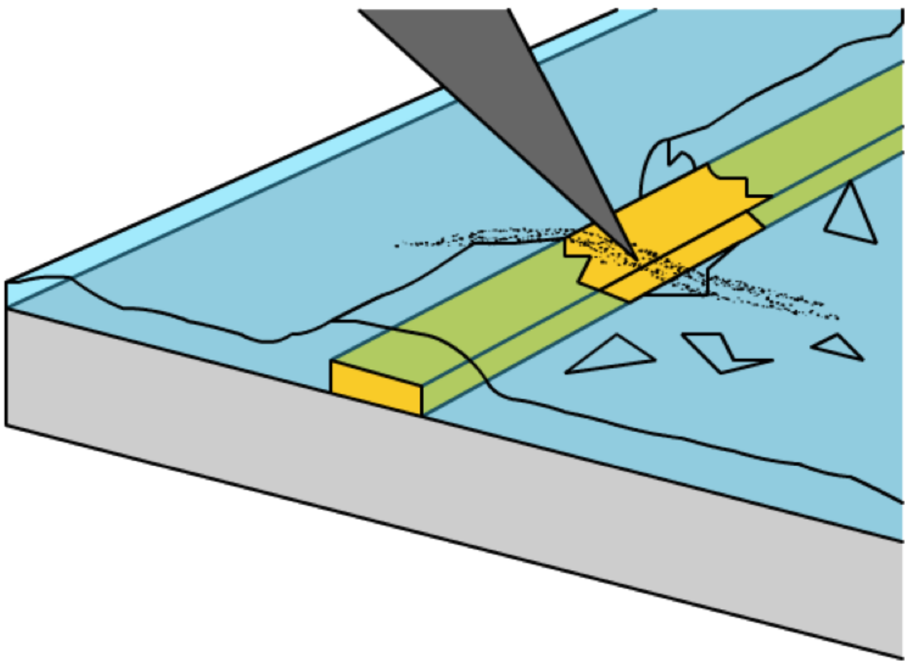
Option B – **Chemically etch into package**

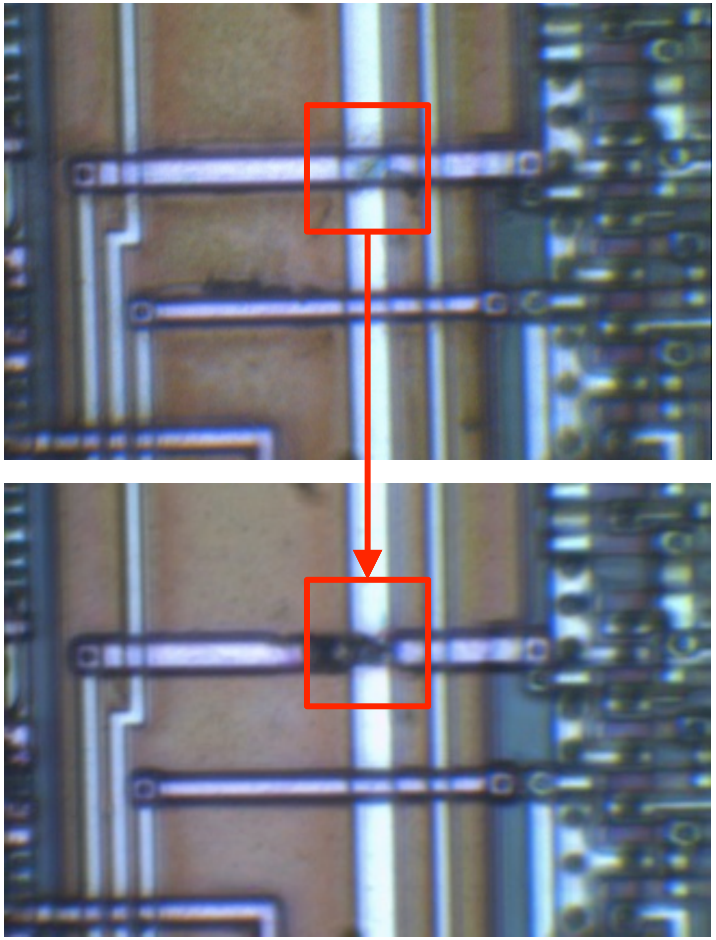


Step 2: Expose wires (1/2)

Option A – **Scratching**

- A micropositioner in combination with hard needles can break the silicon oxide (aka glass) above metal tracks
- Works best for highest ("top") metal layer on non-planarized chips

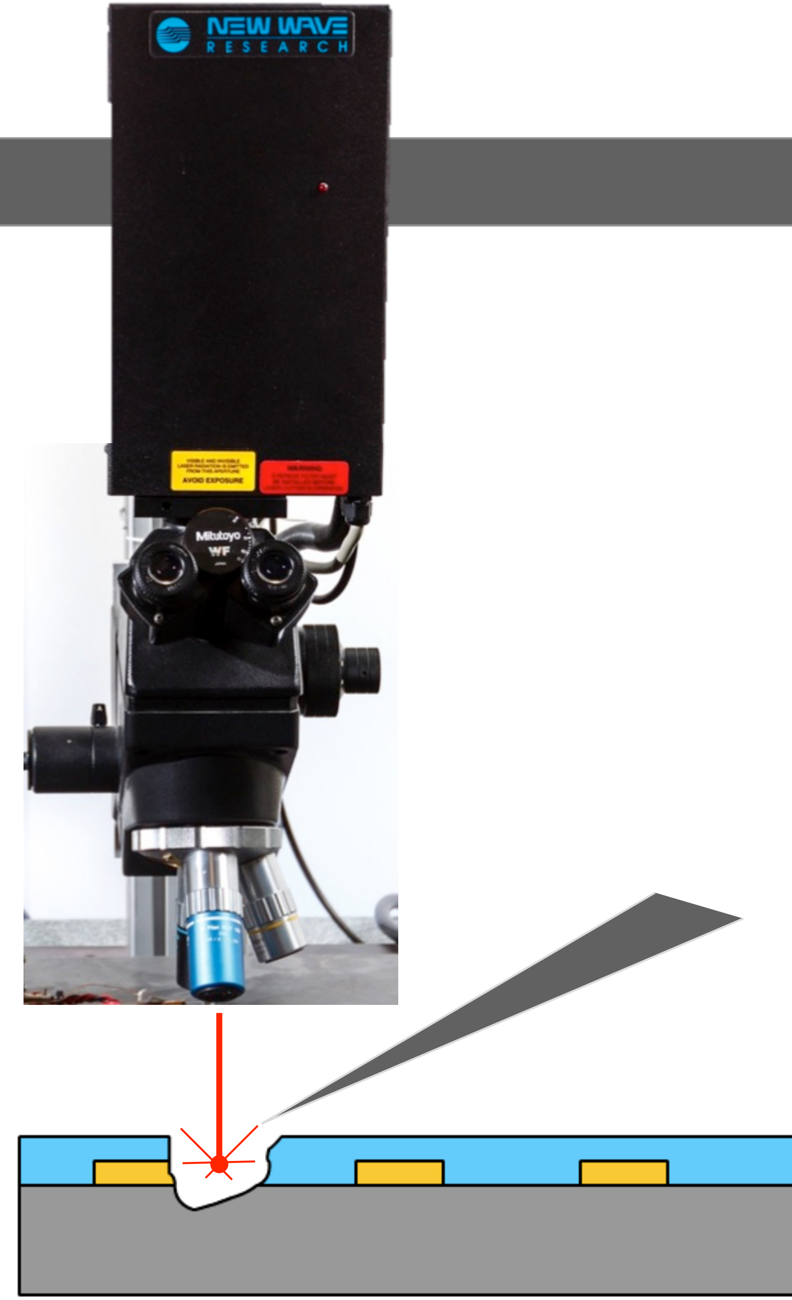




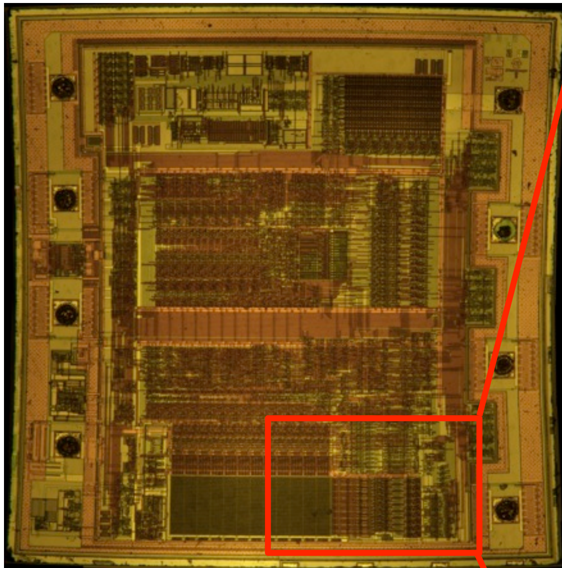
Step 2: Expose wires (2/2)

Option B – **Lasering**

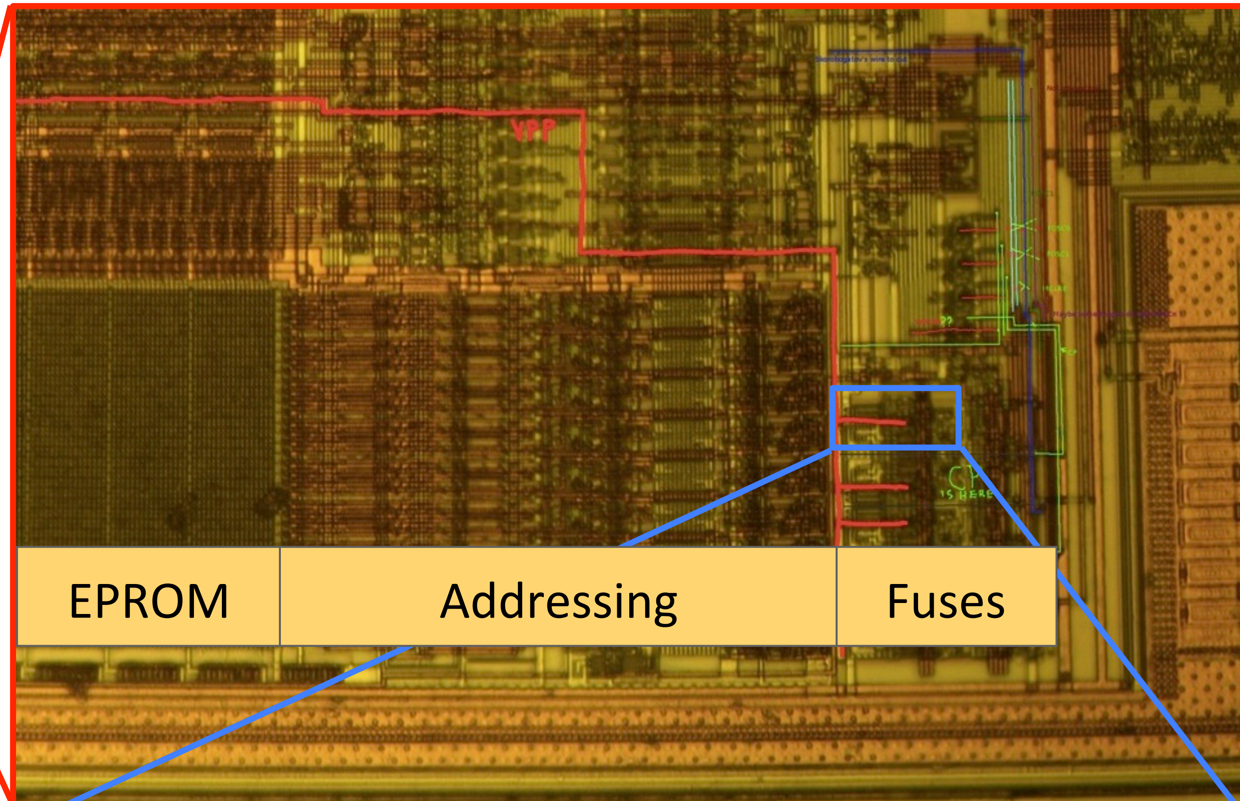
- A laser shot through the microscope destroys chip structures to:
  - Expose wires for probing -or-
  - Cut wires to alter chip logic; i.e. permanently reset lock bit
- Optimal for planarized chips and for working on top metal
- Takes practice to not destroy chips through shorting wires or inducing overvoltage
- Higher cost alternative when compared to scratching but more reliable after practice

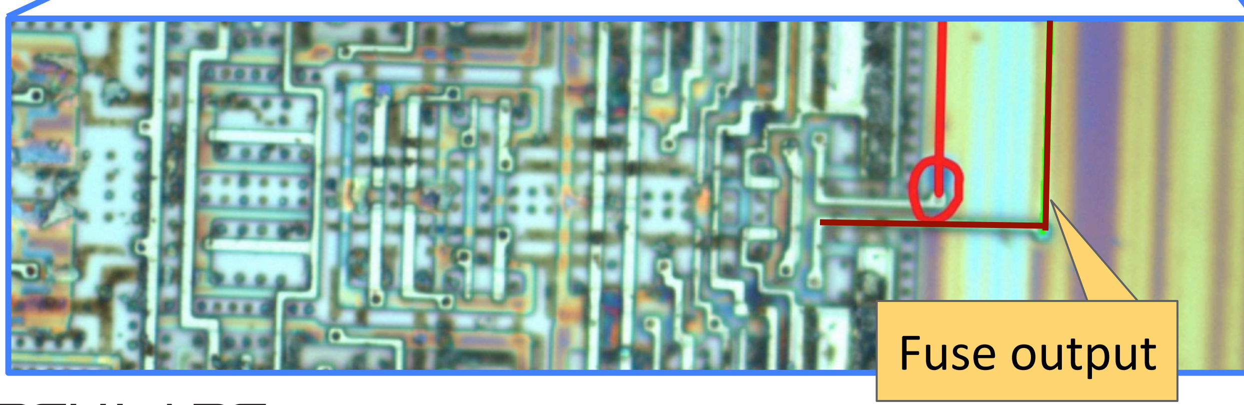


Step 3: Find exploitable wires

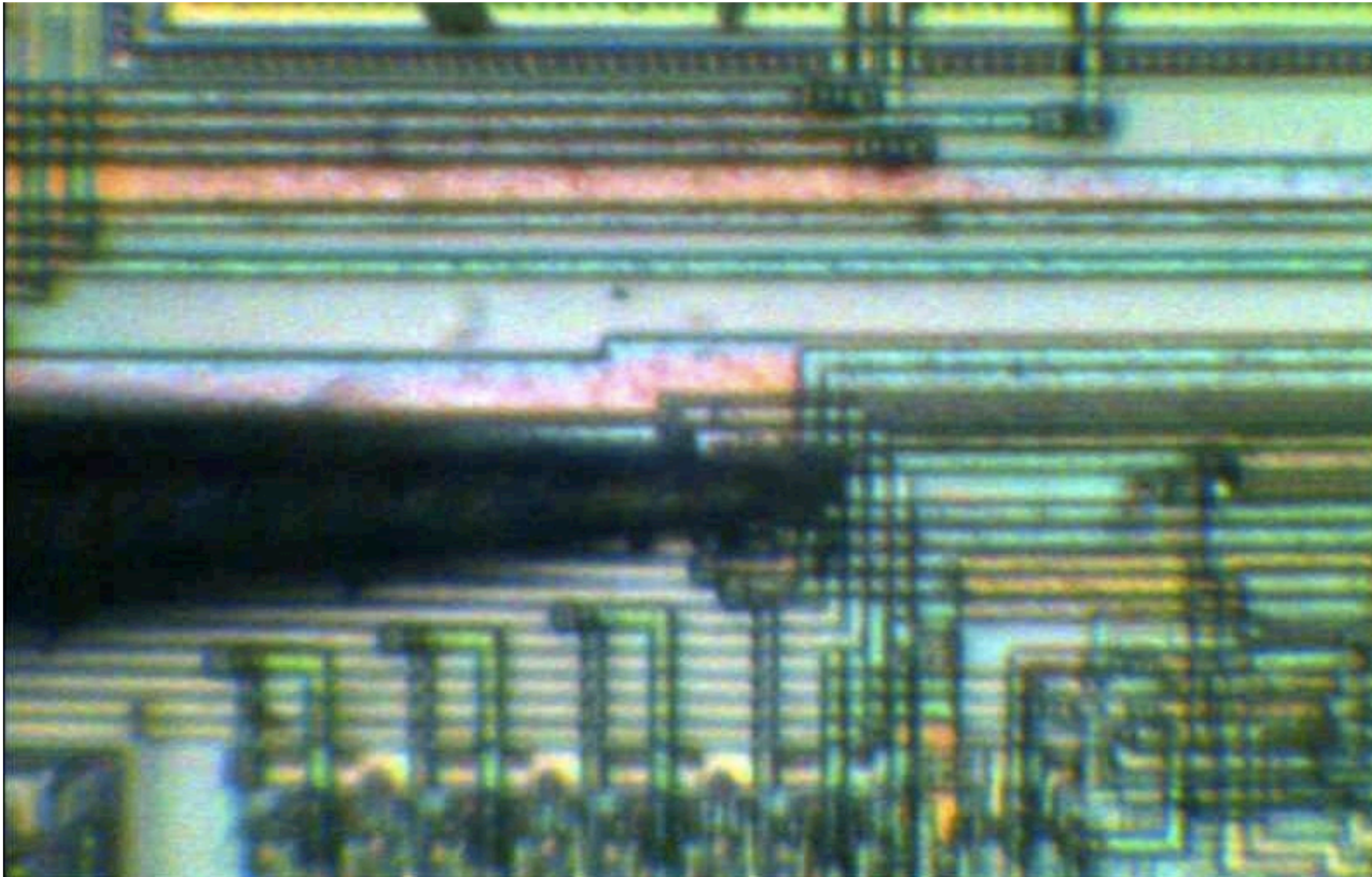


- Most interesting chip structures:
  - Security bits (fuses)
  - Data buses
- Discover them:
  - Reverse-engineer (HAR 09, Camp 11)
  - Trial and error

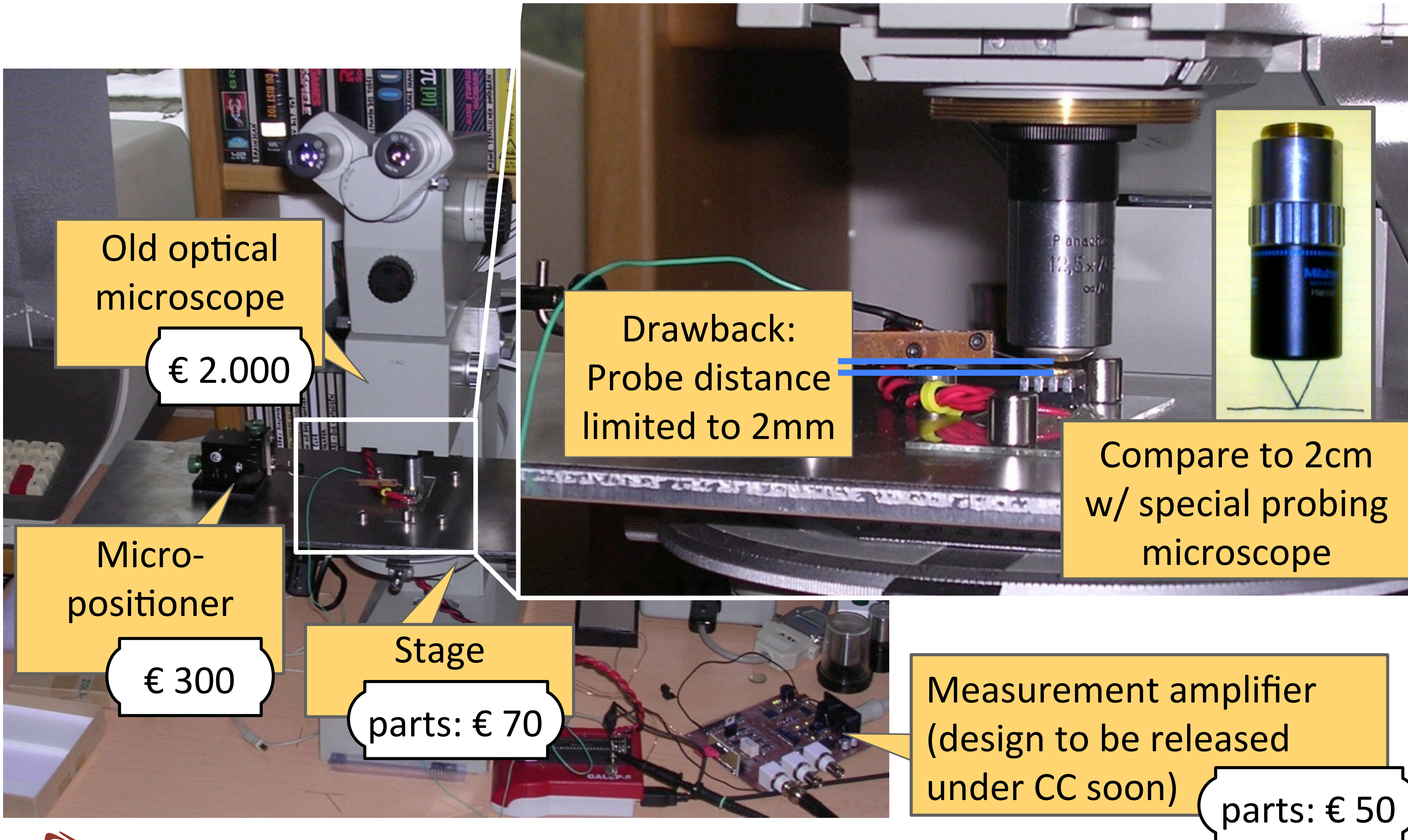




Step 4: Connect to wires with probing needle

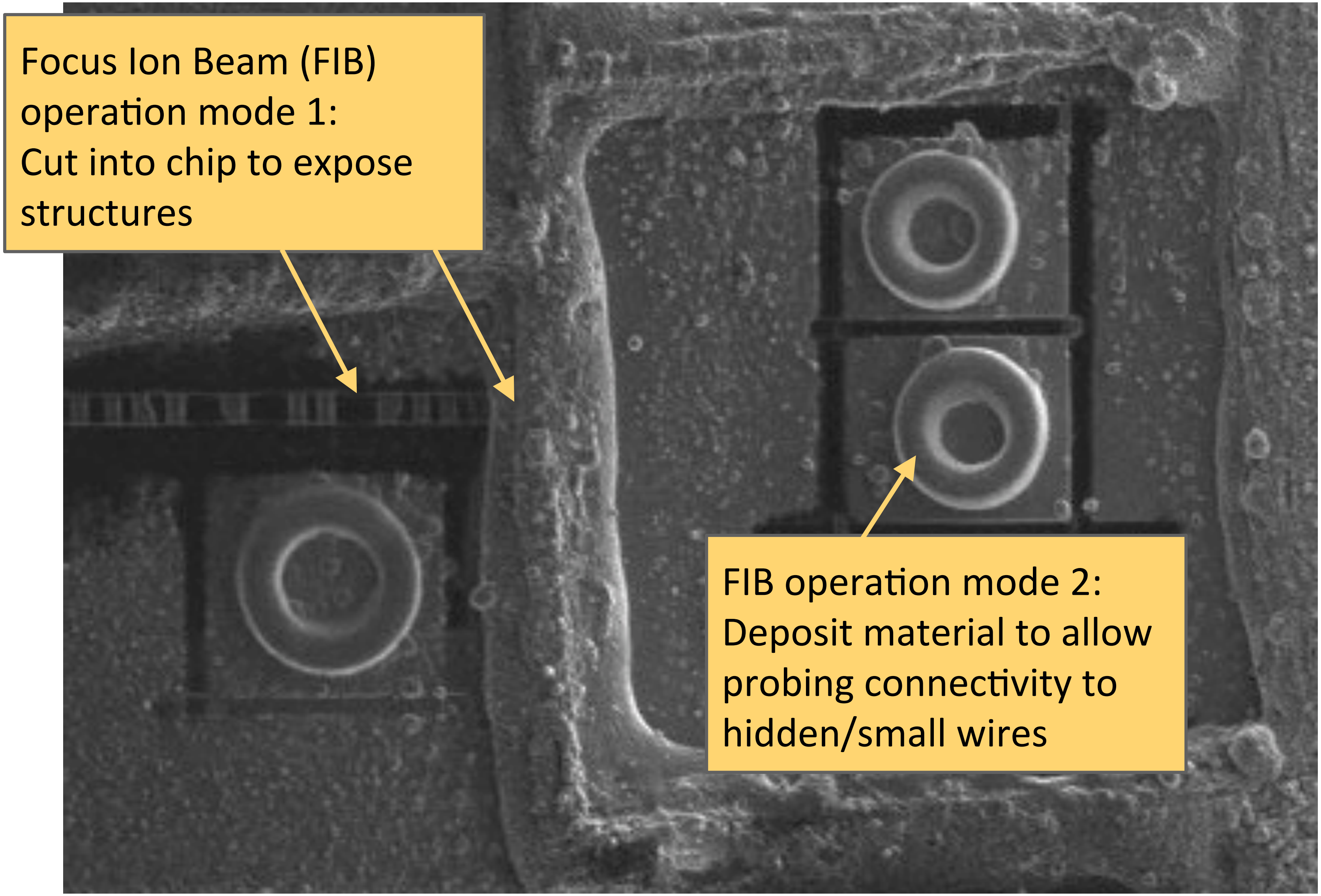


Some level of probing can even be done with simple optical microscopes and few extra components



- Microprobing background
- Probing with simple tools
- **Advanced probing techniques**

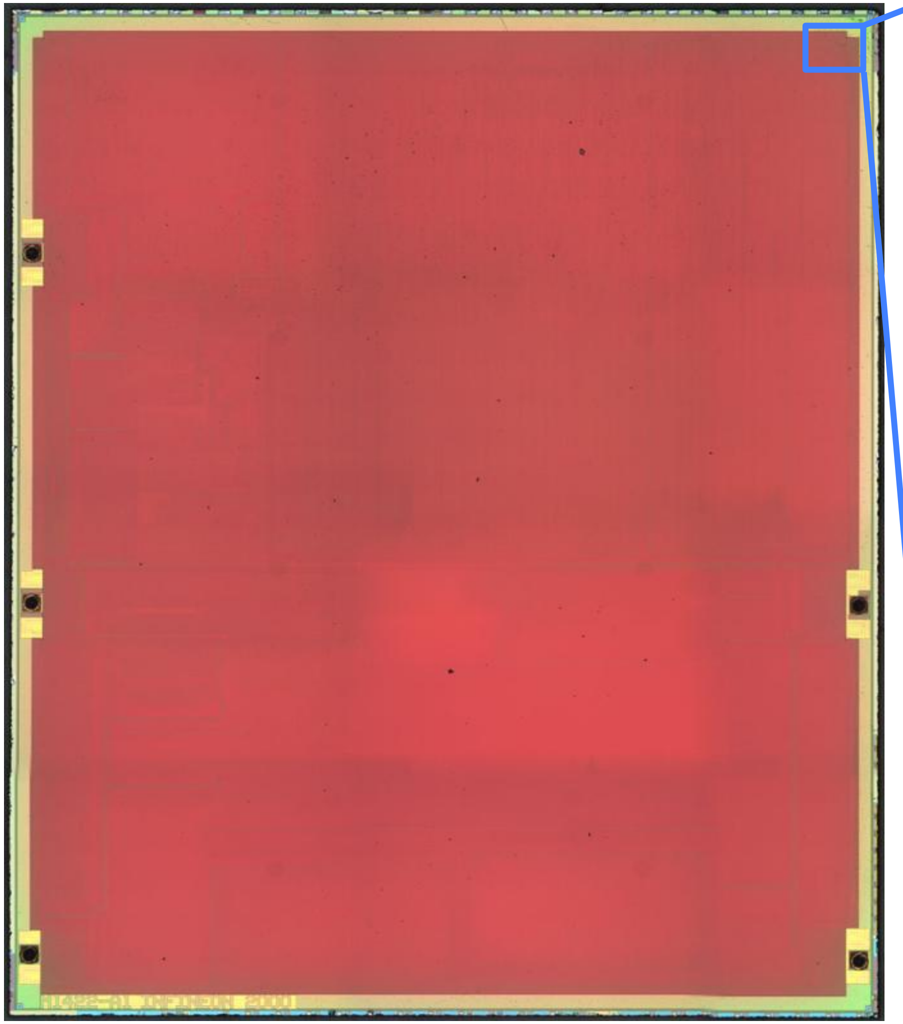
Focused Ion Beams prepare small feature-size chips for probing

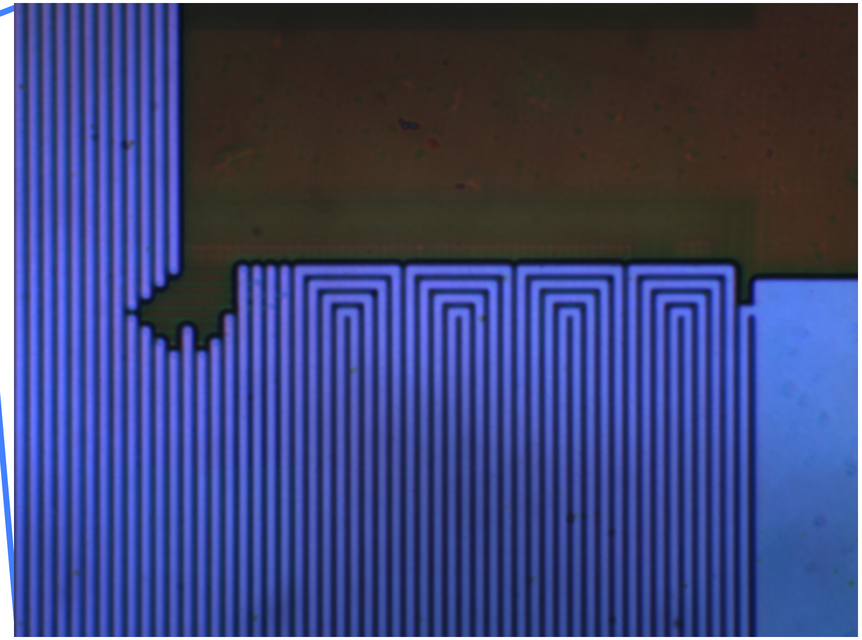


SECURITY RESEARCH LABS

Source: Chris Tarnovsky, Flylogic

Protection meshes create additional complexity for FIB probing

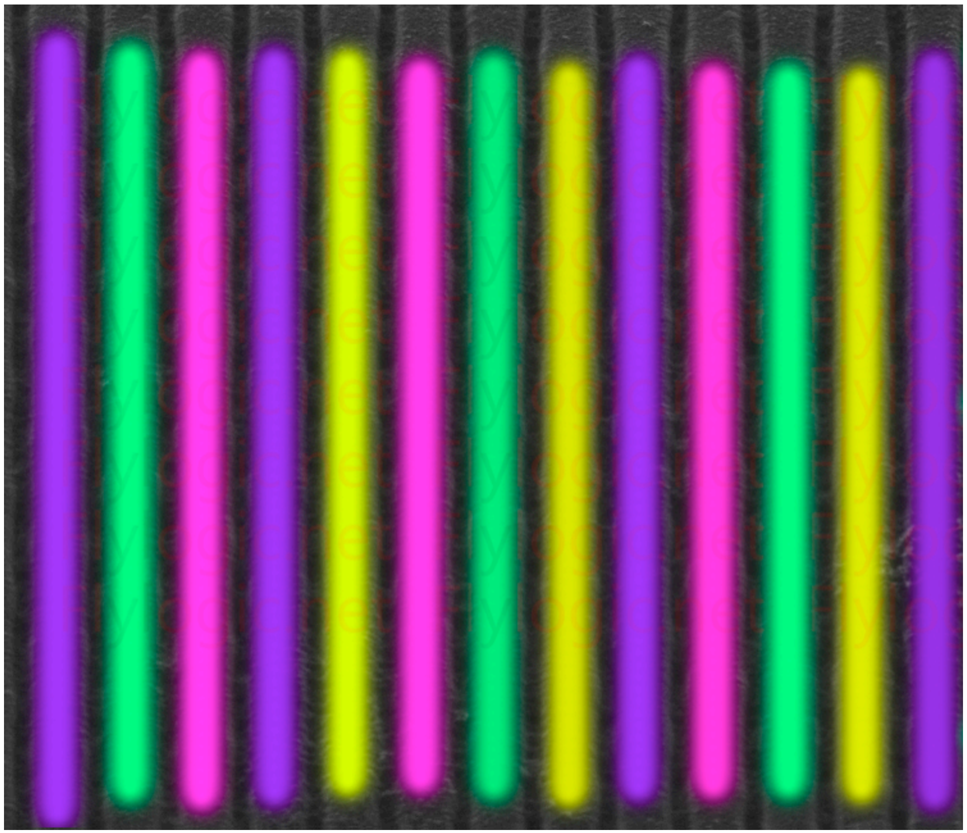




Protection meshes

- Tight metal trace on top layer hides critical structures
- Mesh breach triggers “alarm”

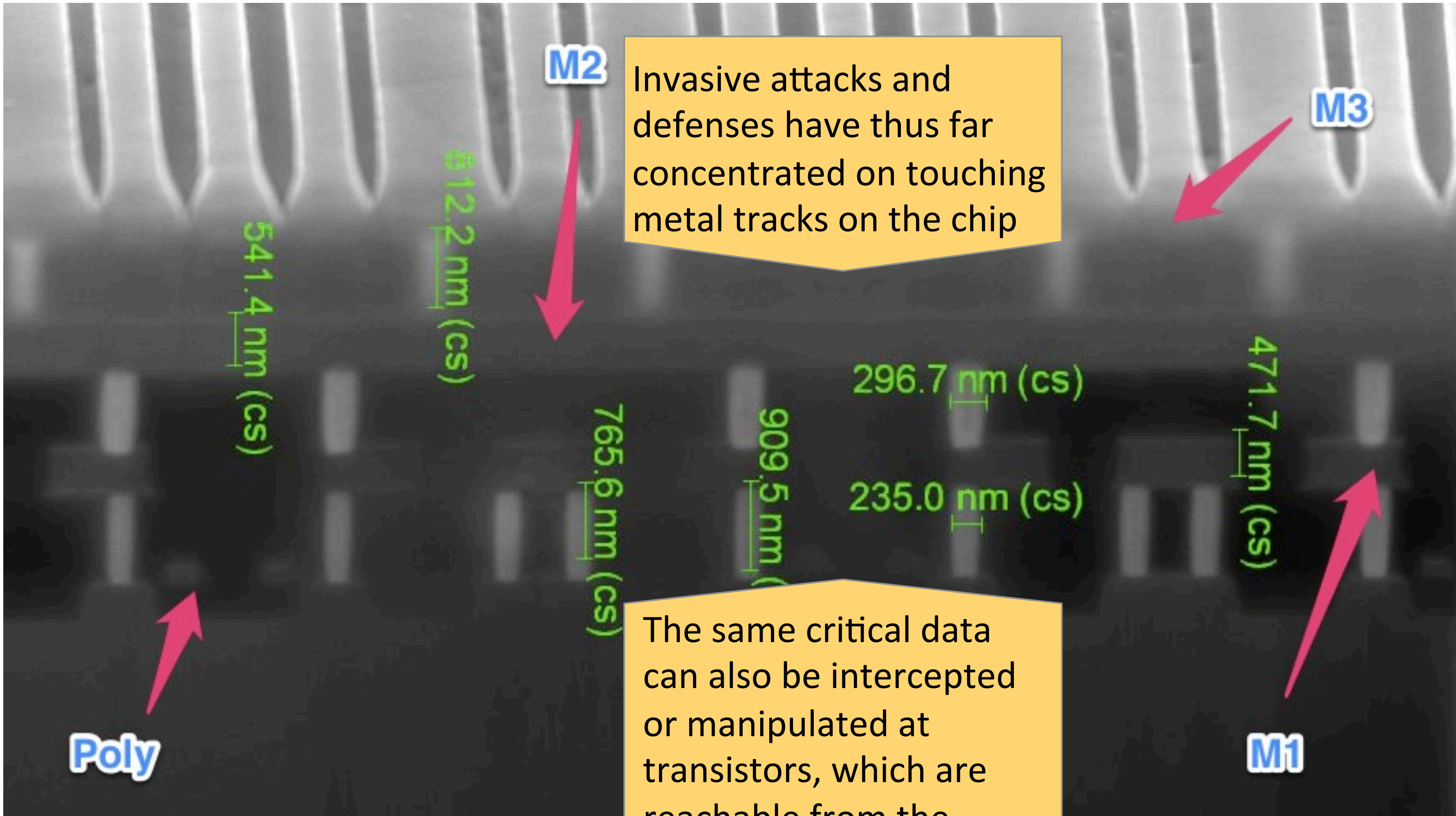
Meshes slow down attack, but do not prevent them



Mesh circumvention

- Either remove parts of mesh, then bridge/fix the mesh with FIB edits -or-
- Circumvent mesh alarm:
  - If defense is bulk-erase of non-volatile memory: Cut off the programming pumps
  - If chip it is logic reset: Exploit in the small time window before the reset triggers

Arms race around front-side FIB attacks makes back-side attacks more attractive



Invasive attacks and defenses have thus far concentrated on touching metal tracks on the chip

The same critical data can also be intercepted or manipulated at transistors, which are reachable from the other side of the chip

Take aways

- Device functionality is increasingly hidden in hardware and needs to be freed

- Software can be extracted from chips using fuse overwrites or linear code extraction

- Simple controllers can be attacked with cheap tools; smart cards require focused ion beams

Questions?

Philipp Maier <dexter@srlabs.de>
Karsten Nohl <nohl@srlabs.de>