CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 15: Anti-tamper technologies

Homework 2: PCB RE

- Due last day of class
- Go to one of the tech dumps and find a PCB
- Take photos of both sides, both overview and closeups of interesting areas
- Identify as many ICs as you can
- Draw a block diagram of the board and write a short report describing its functionality

Types of defenses

- Non-invasive protections
  - Lock bits, glitch detection
- Semi-invasive protections
  - Metal shielding
- Invasive protections
  - Die coats
  - Meshes
- Self-destructs

Lock bits

- Threat: Non-invasive memory dumping
- Config bit(s) set in firmware image
- Inhibit some operation when set
  - All JTAG operations
  - Debug port
  - Firmware readback
  - Erase/reprogram (use with care, can brick)

Lock bits

- Dedicated NVRAM (PIC12F)
  - Typically weaker - more vulnerable to UV etc
- Embedded in firmware flash (XC2C32A)
  - Can be easy to find if address map is known
  - Sometimes harder to tamper with

Glitch sensors

- Threat: Glitch/fault attacks
- Sensors to detect abnormal conditions
  - Fclk out of range
  - Vcore out of range
  - Temp out of range

Optical sensors

- Threat: Any attack involving opening package
- Scatter unshielded phototransistors around
- Trigger when illuminated
- May not detect laser glitching in a dark room

Glitch/optical sensors

- Can only detect specific fault conditions
- Will do nothing against other attacks
- Can sometimes be bypassed
  - ex: black ink over light sensors

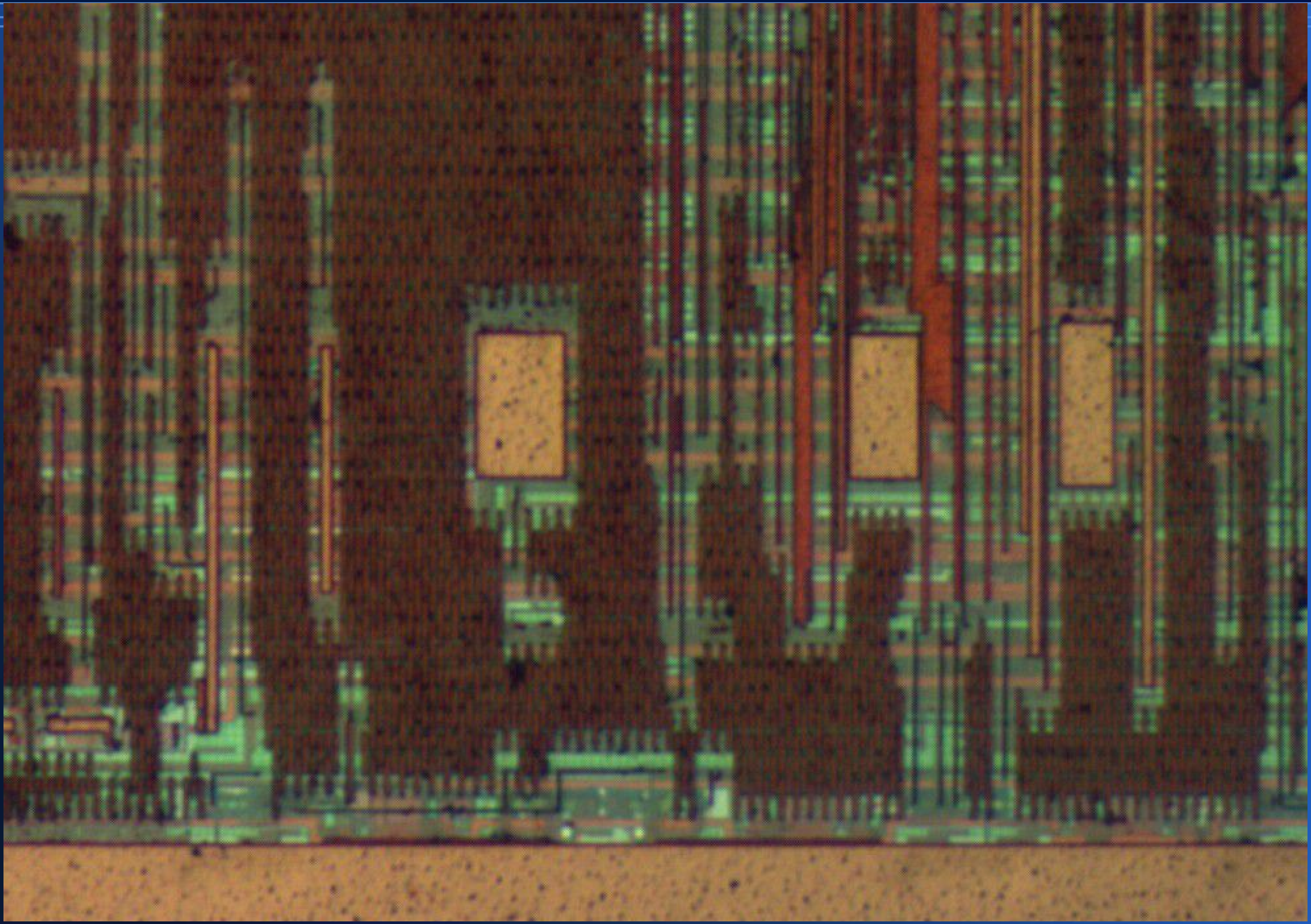
Power noise generation

- Threat: Power analysis
- Random number generator plus variable load
- Induce random power fluctuations to confuse analysis
- Must be higher freq than sensitive power trace and completely unpredictable

Optical shielding

- Threat: UV erasure
- Place lots of big opaque metal polygons over fuse/memory areas

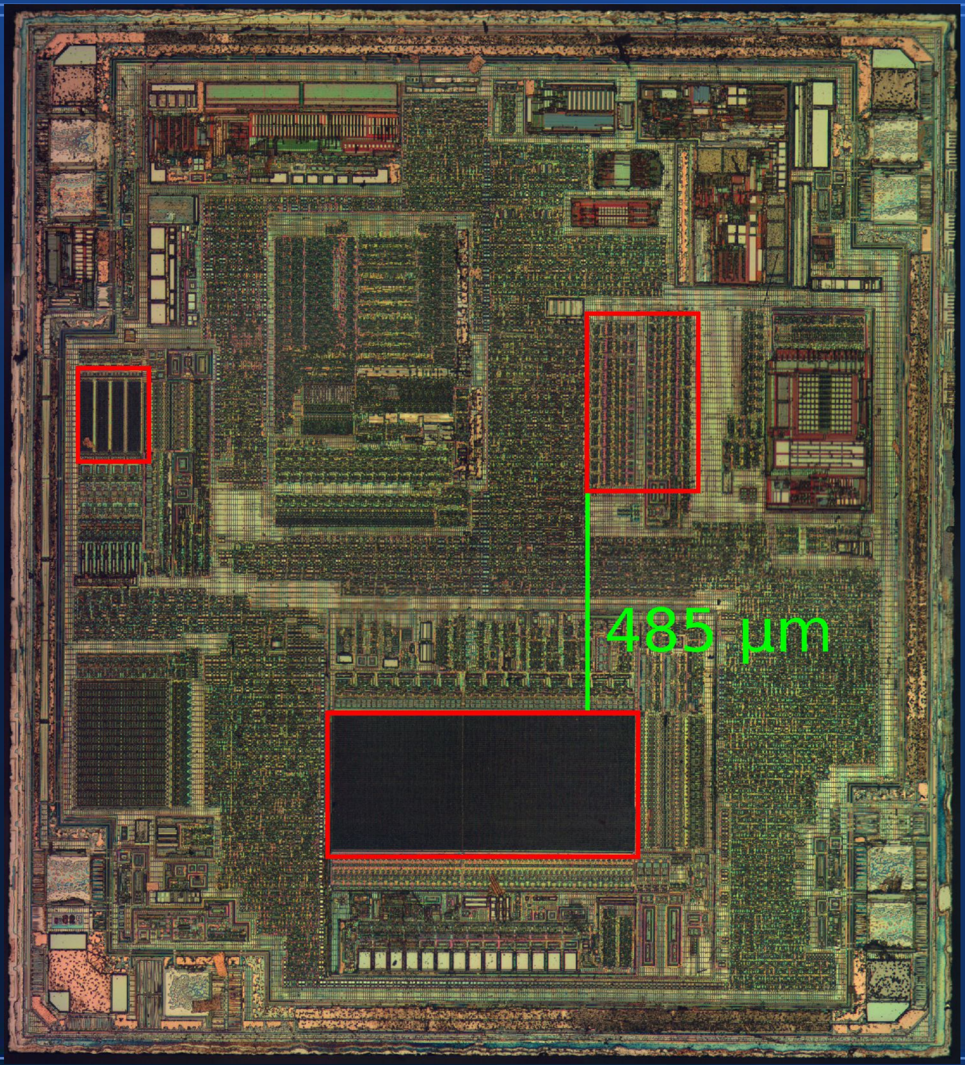
Optical shielding

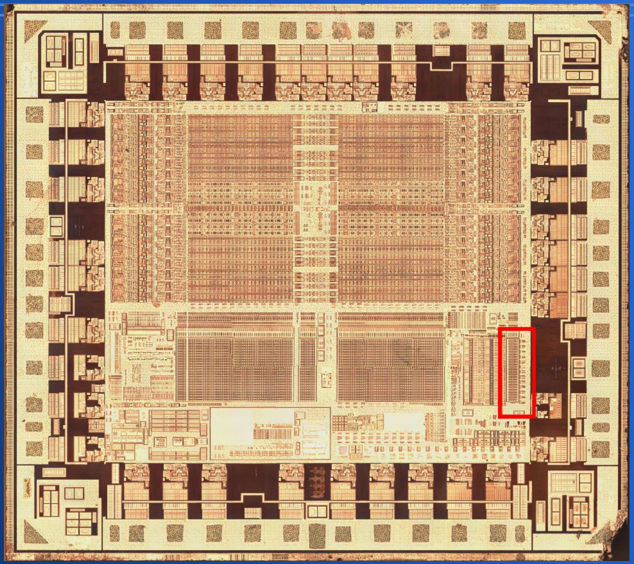


Placement

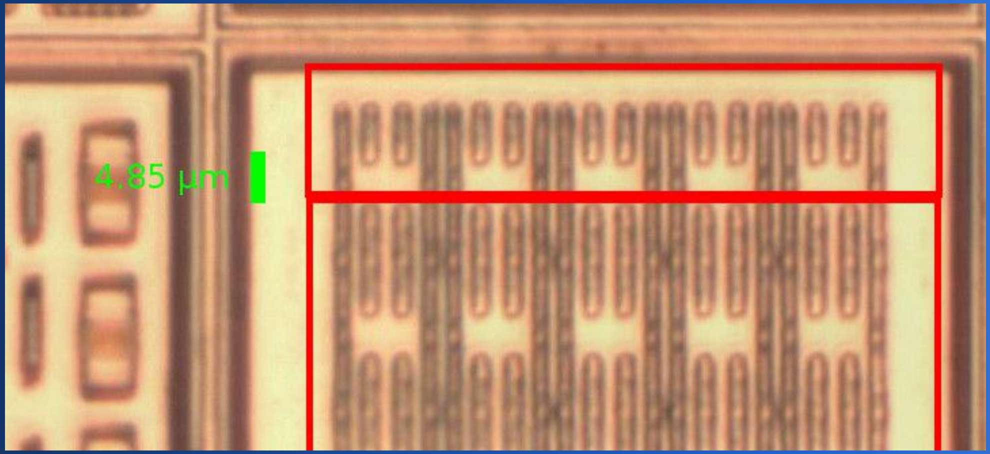
- Place features likely to be tampered with next to critical data
- Ex: interrupt vector address right next to security bits
- UV attack etc is more likely to damage both

PIC12F683 vs XC2C32A





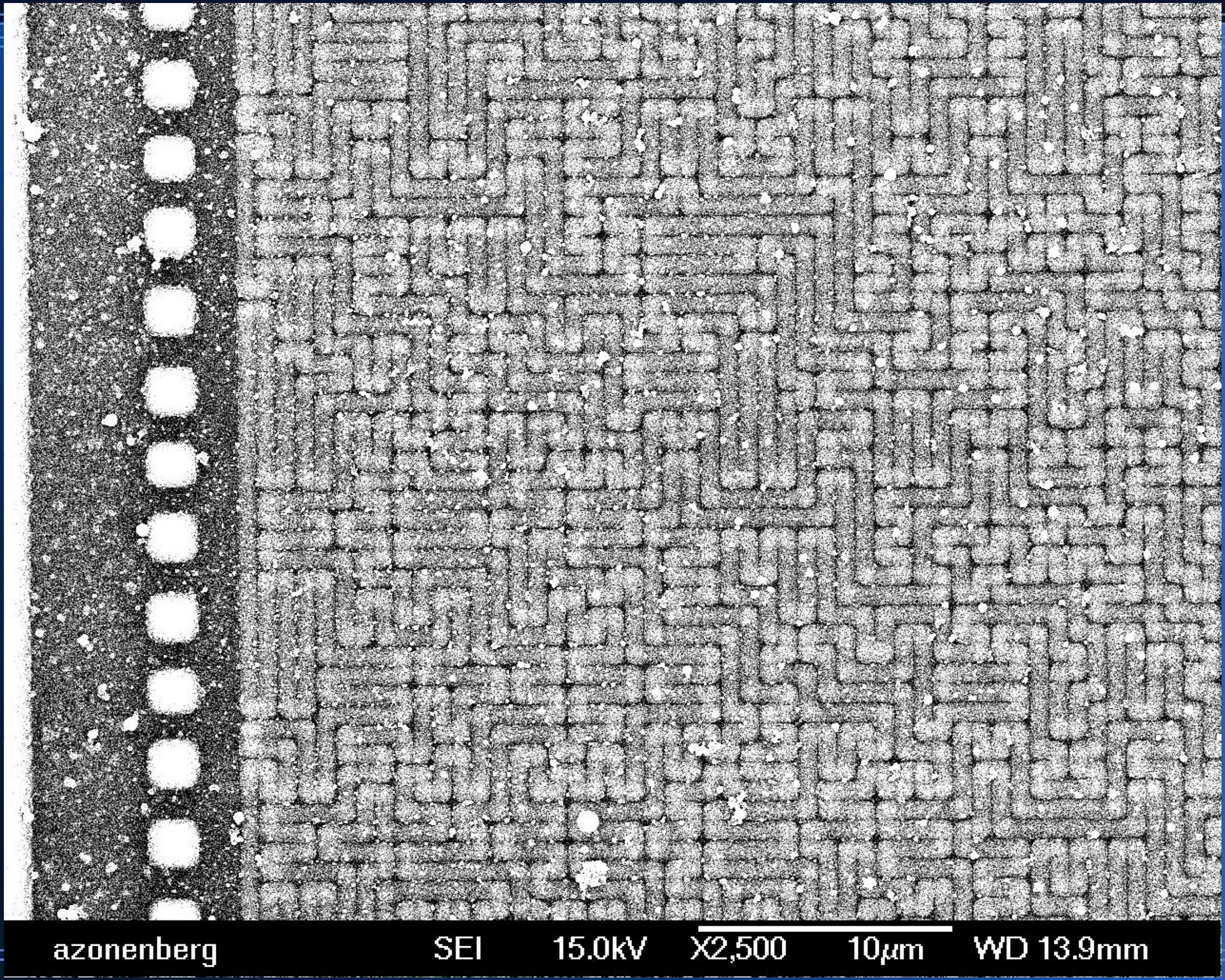
100x closer!



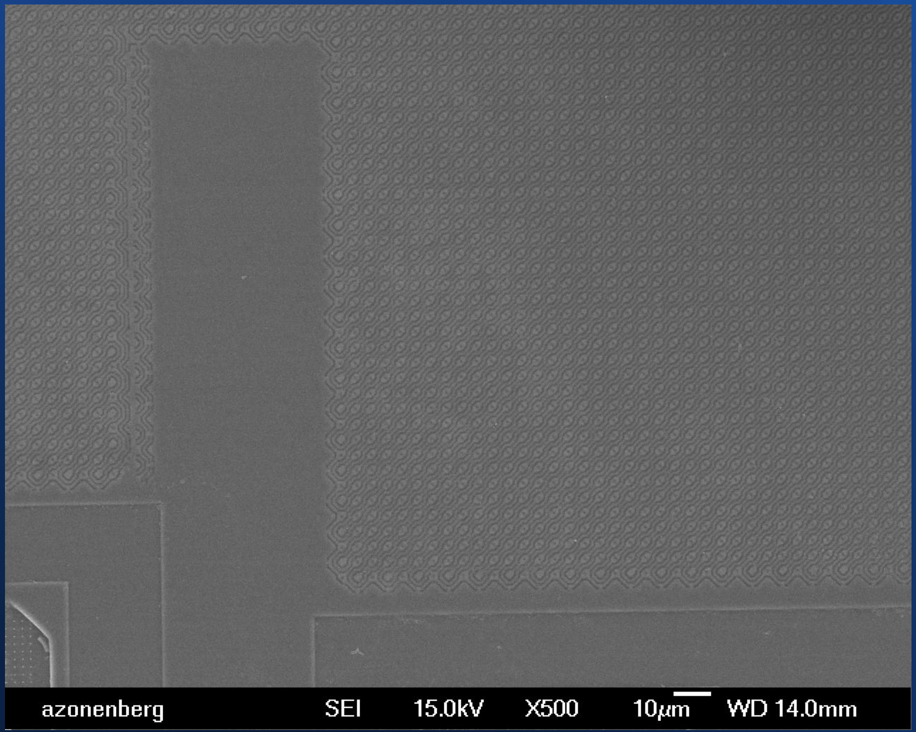
Active meshes

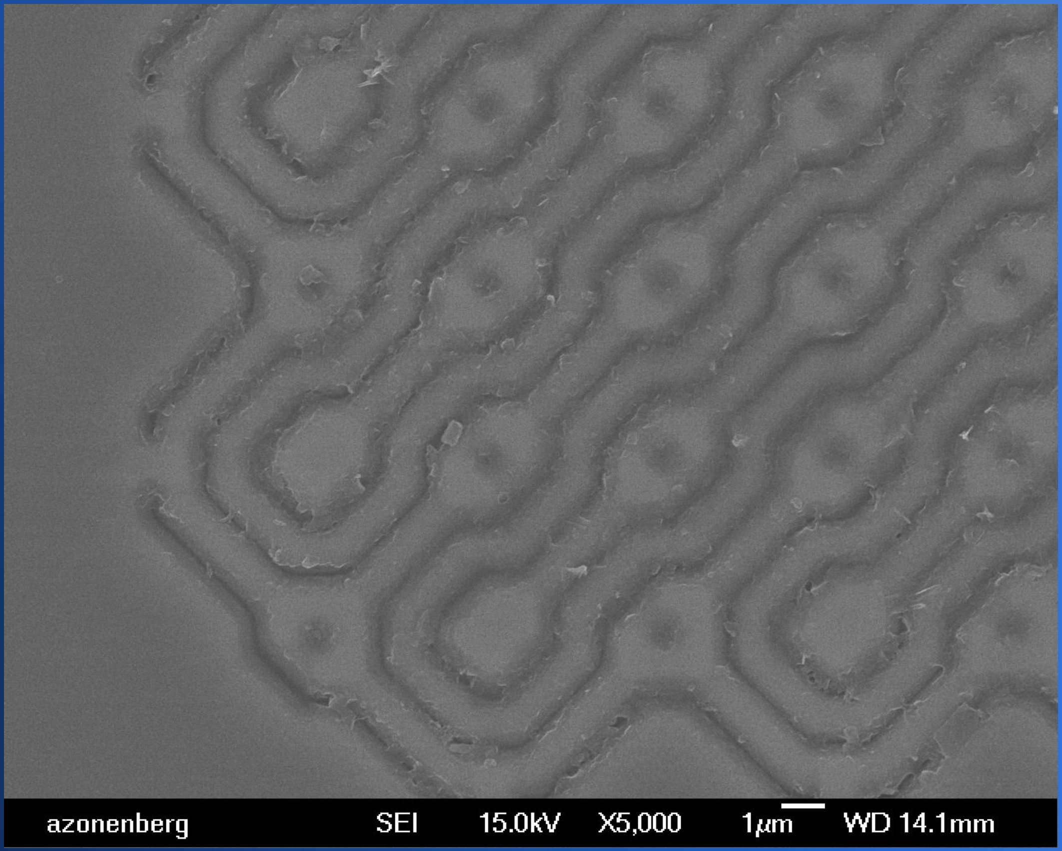
- Fill the top surface of the die with wire(s) forming a space-filling curve
- Alarm if the wire is broken, or if two signals short together
- Effective at preventing physical probing
- Also blocks top signal layer from visual inspection

Active mesh (Atmel ATSHA204)

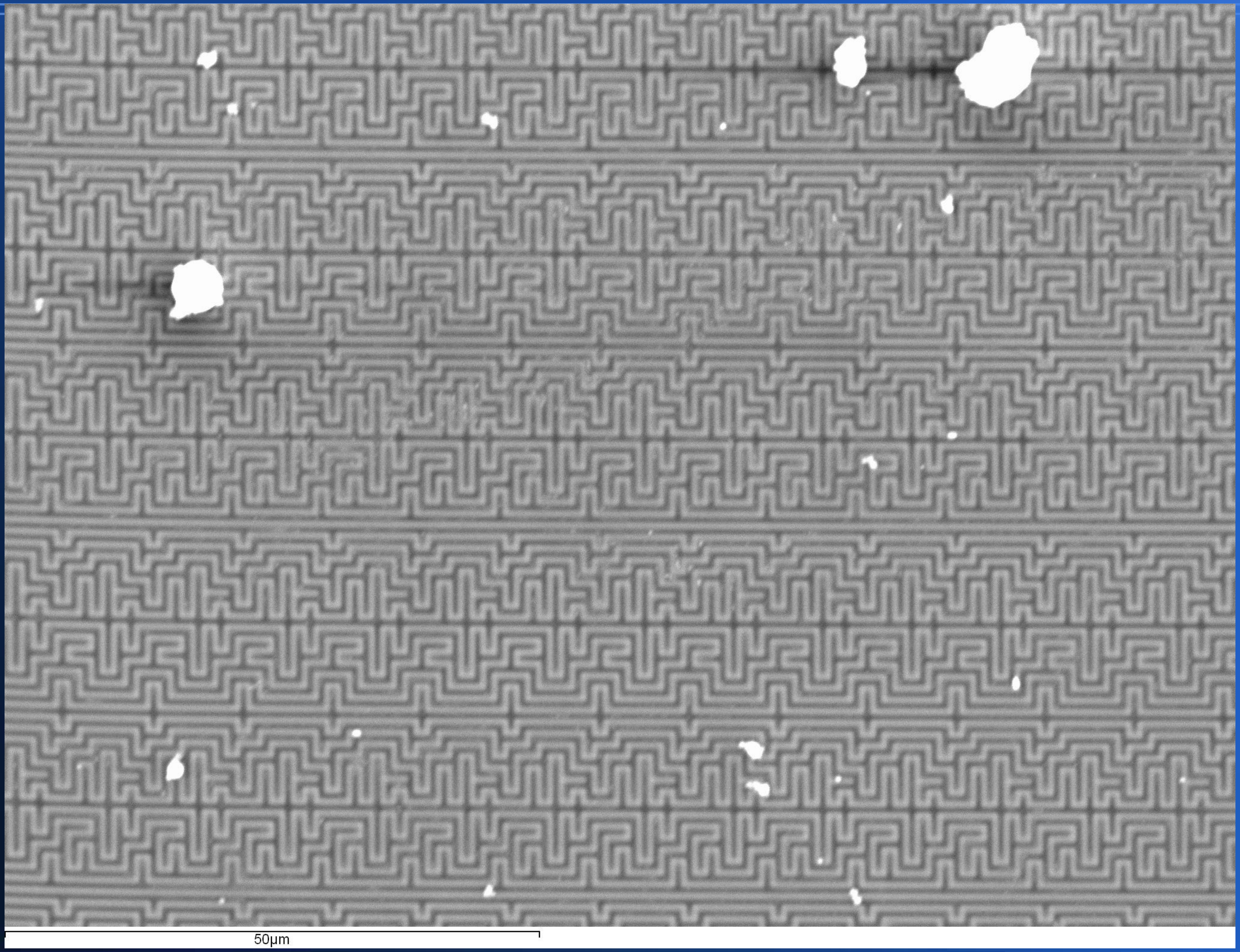


Active mesh (ST K710A)

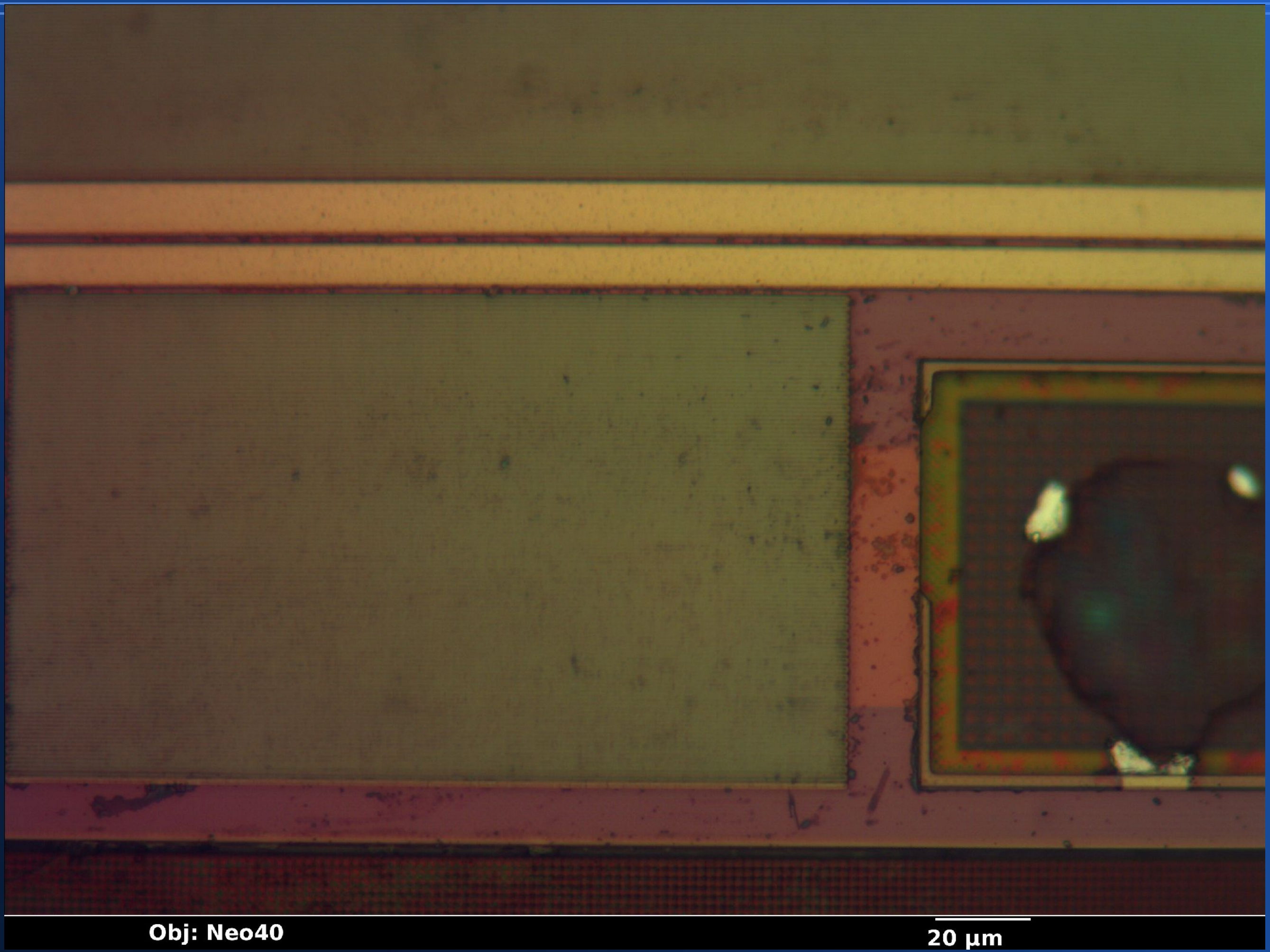


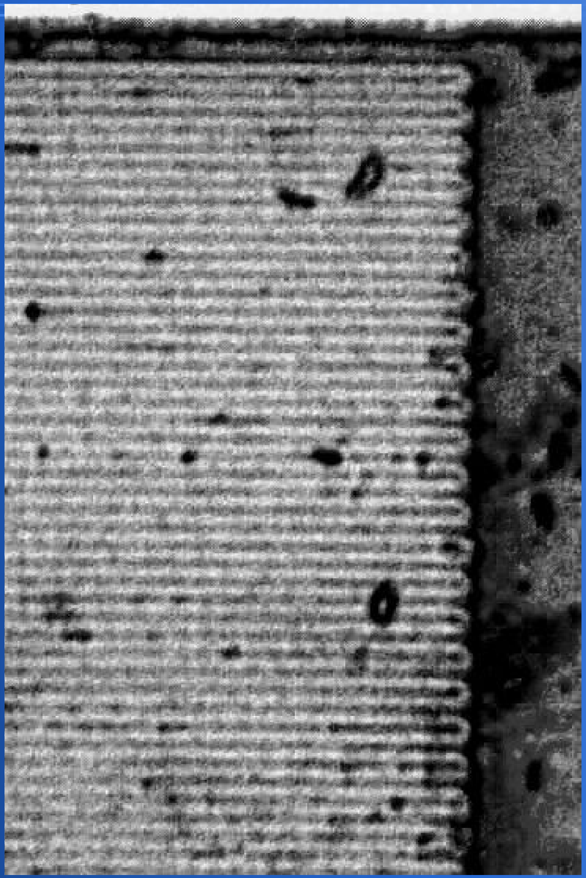


Active mesh (Renesas R5H30201)



Active mesh (AT&T SIM card)





Mesh bypass

- Several possible attacks
- Use FIB to nick (but not cut) mesh and edit underlying layers
- Remove mesh entirely and tie sense lines off
- Cut/gate mesh sensor output
- Go in from back side and avoid mesh entirely
- Etch/laser cut mesh and reconnect with probes
  - Works OK if not too many lines

Class discussion

- Which of the meshes shown do you think is most secure? Least? Why?

Tamper responses

- Freeze (gate clock)
- Reset
- Self-destruct (erase firmware/data/keys)

Self-destructs

- Flash erase
  - Can be prevented
  - Laser/FIB/etch out charge pump caps
  - Cut/short write enable lines, HV outputs, etc
  - No HV = no writes
- Zeroize battery-backed SRAM
  - Much harder to prevent

Extreme countermeasures

- Mostly used in military devices? We have not see any of these in commercial products
  - Connoisseur Coating
  - LOPPER

Connoisseur Coating

- Developed by LLNL as part of the “Connoisseur project”.
- Very little public information
- http://www.nytimes.com/1989/11/08/business/business-technology-a-new-coating-thwarts-chip-pirates.html
- http://web.mit.edu/6.857/OldStuff/Fall95/lectures/lecture2.ps

1989 New York Times article

- “A resin about the consistency of peanut butter”
- “Opaque and resists solvents, heat, grinding and other techniques”
- “A second-generation coating is being developed that will automatically destroy the chip when an attempt is made chemically to break through the protective layer.”

1995 MIT lecture slides

- The second-generation coating?
- “a layer of alumina, silicon bits, and even sodium coating”
- “usually expensive”

Weaknesses of die coatings

- Intention is to make it difficult or impossible to reach top die surface
  - None of the public materials mention any protections on the back side
  - Die substrate is normally pretty thick, can handle some scratching
  - Backside attacks may allow coating bypass

LOPPER

- Developed by NSA for VINSON
- Not deployed initially due to budget cuts
- Plant “tiny, non-violent, shaped charges in critical junctures in our circuits that could be triggered by the application of external voltage”
- [A history of US COMSEC, page 148]

LOPPER v2?

- “burying a resistor in the chip substrates which will incinerate micro-circuitry with the application of external voltage”
- [A history of US COMSEC, page 149].

Possible LOPPER sighting?

- A large rock in Iran near a nuclear site exploded in 2012 when moved, throwing fragments of destroyed PCBs around
- http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?hp&_r=2

Attacks on LOPPER

- “Iranian Embassy” attack
  - If explosive charges are poorly placed, fragments may still yield useful circuit info
  - Collect shrapnel from several units and reconstruct circuit

Attacks on LOPPER

- “Bomb squad” attack
  - Destroy trigger mechanism
  - Bypass sensors

Questions?

- TA: Andrew Zonenberg <azonenberg@drawersteak.com>
- Image credit: Some images CC-BY from:
  - John McMaster <JohnDMcMaster@gmail.com>