CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 14: Invasive attacks

Attack types

- Semi-invasive
  - Device is depackaged, but die isn't damaged
- Invasive
  - Any attack involving physical damage to die

Semi-invasive attacks

- UV [E]EPROM/Flash erasure
- Laser glitching
- Laser-assisted power analysis

UV memory erasure

- Shield memory to be preserved
  - Apply opaque paint under optical microscope
- Expose target memory to shortwave UV light
  - Unshielded mercury vapor tube is ideal
  - Direct sunlight may work but is a bit slower
- Exposed memory cells should now be “1”

UV memory erasure

- Works with all floating-gate memories
- Serious limitations!
  - Only works one way, cannot set bits to 0
  - Indiscriminate, can't target single bits
- But very easy and inexpensive

Microchip PIC12F683

- 350 nm 3-metal
- 8-bit RISC CPU core
  - 20 MHz / 4 CPI = 5 MIPS
  - 8-level hardware stack

PIC12F683 memory arrays

- 128 bytes SRAM
- 256 bytes data EEPROM
- 2048 words flash
- 12 bit configuration register

Configuration memory map

- 0000 - 07FF = firmware flash
- 2000 - 2003 = user ID code
- 2006 - 2006 = device ID (ROM)
- 2007 - 2007 = config word
- 2008 - 2008 = calibration word
- 2100 - 21FF = data EEPROM
- Other locations non-implemented

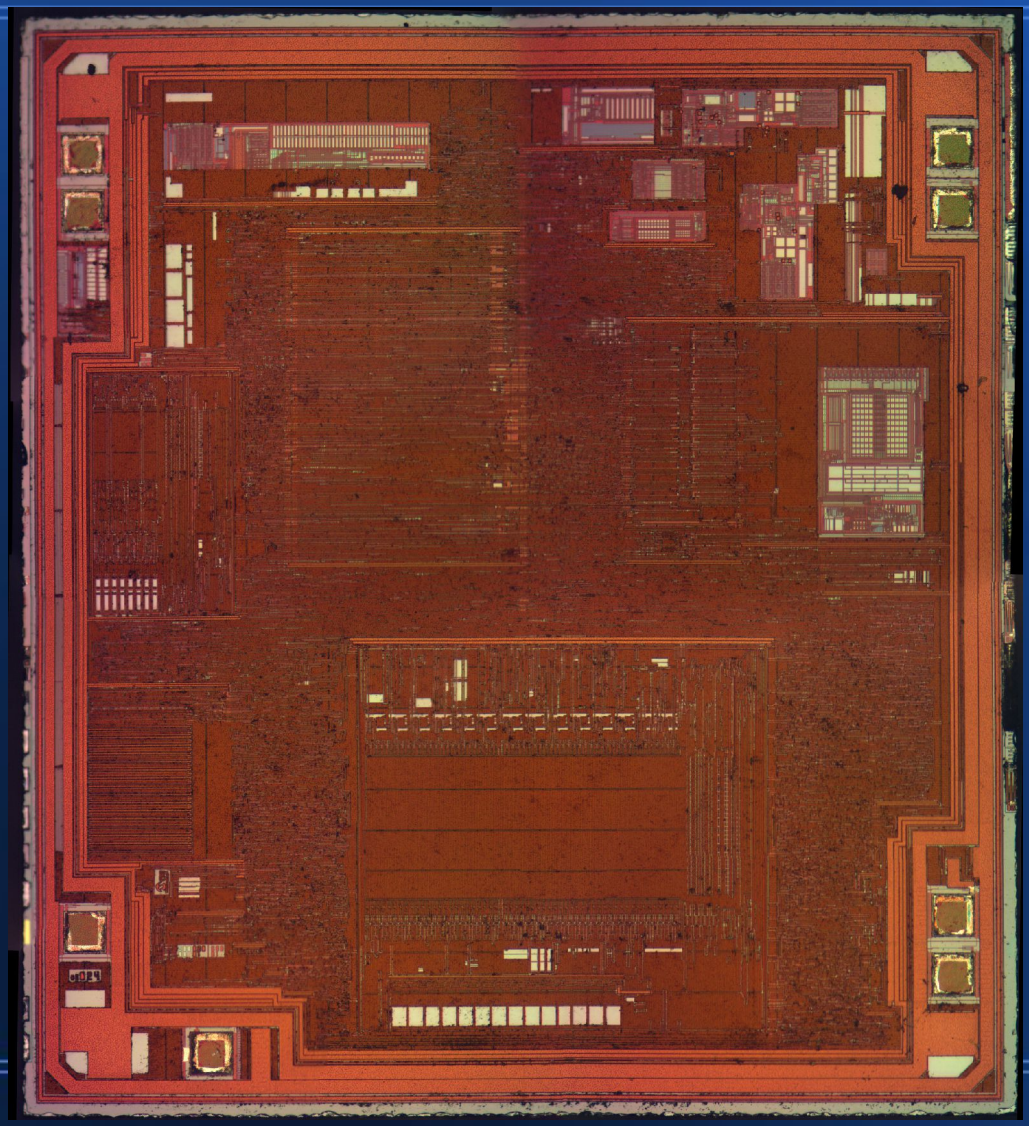
Configuration register

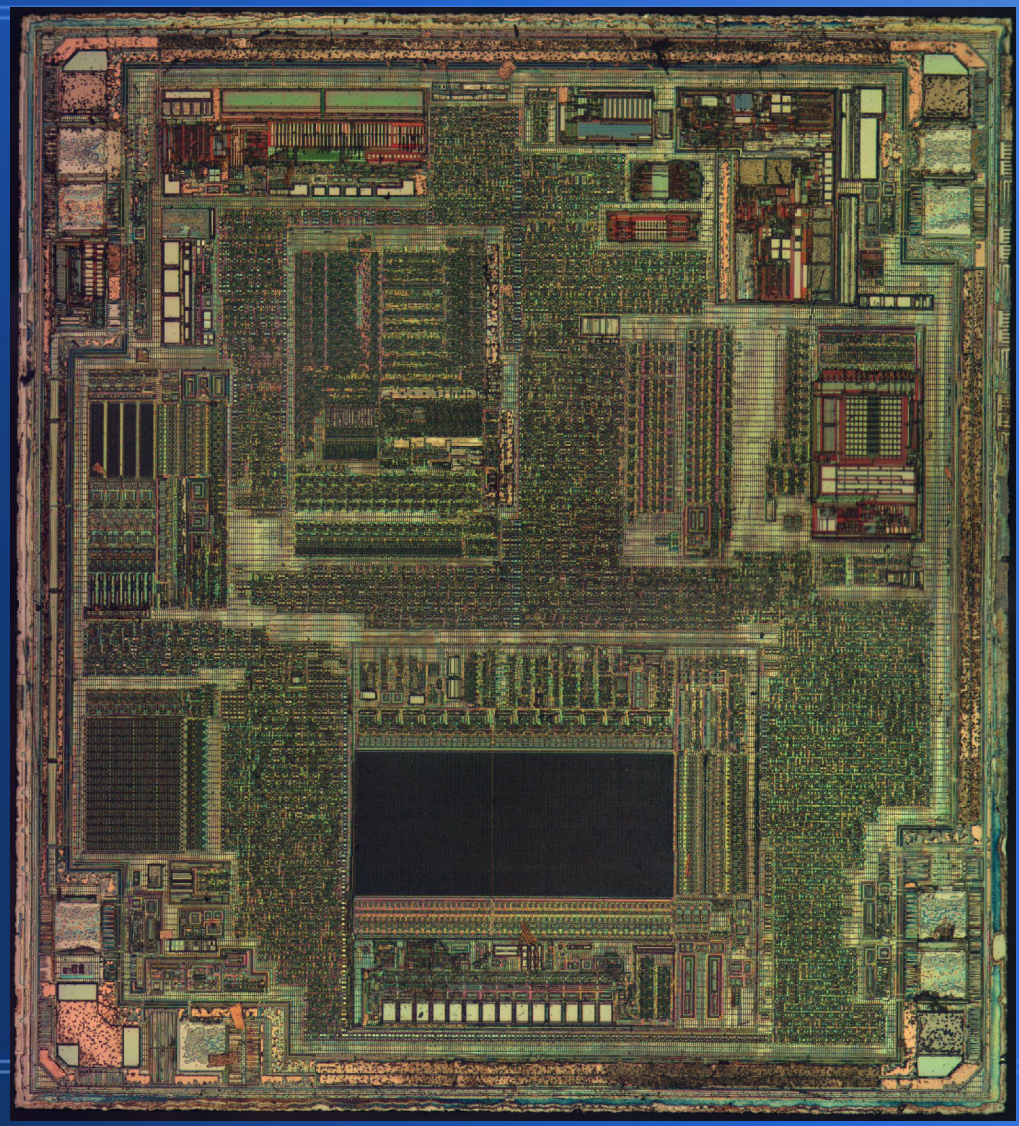
- Stored at word address 0x2007
  - Byte address 0x400e
- Boot configuration stuff
  - Several bits related to clock sources, resets
  - CONFIG[7] = CPD# (read lock on EEPROM)
  - CONFIG[6] = CP# (read lock on flash)
  - If bit is 1, can read back over ICSP
  - If bit is 0, readback gives all zeroes

Configuration register

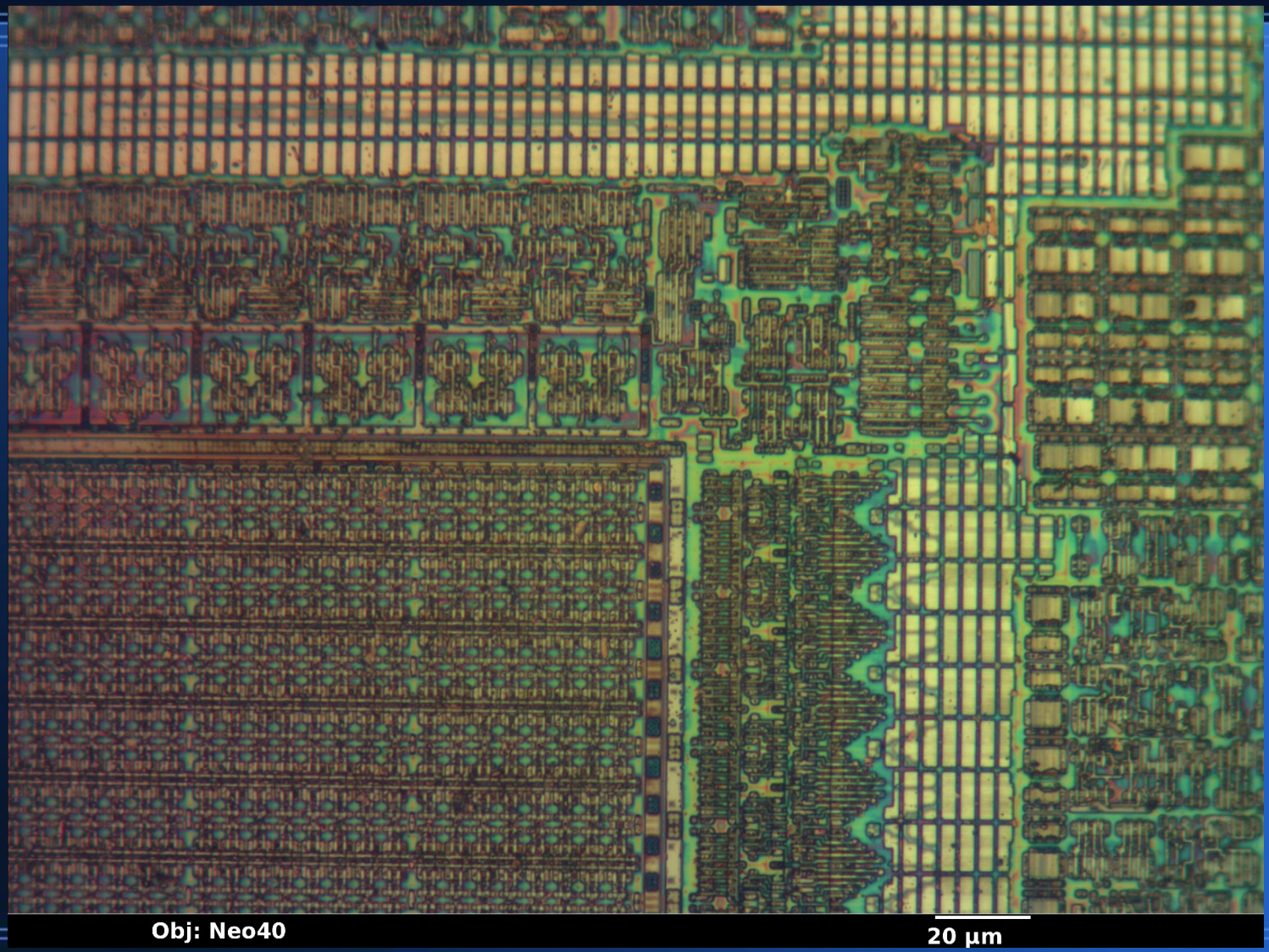
- Older UV EPROM PICs needed “1” = unlocked
- Modern parts (at least up to 350 nm) kept this
  - Susceptible to UV light attacks!

PIC12F683 M3 and poly

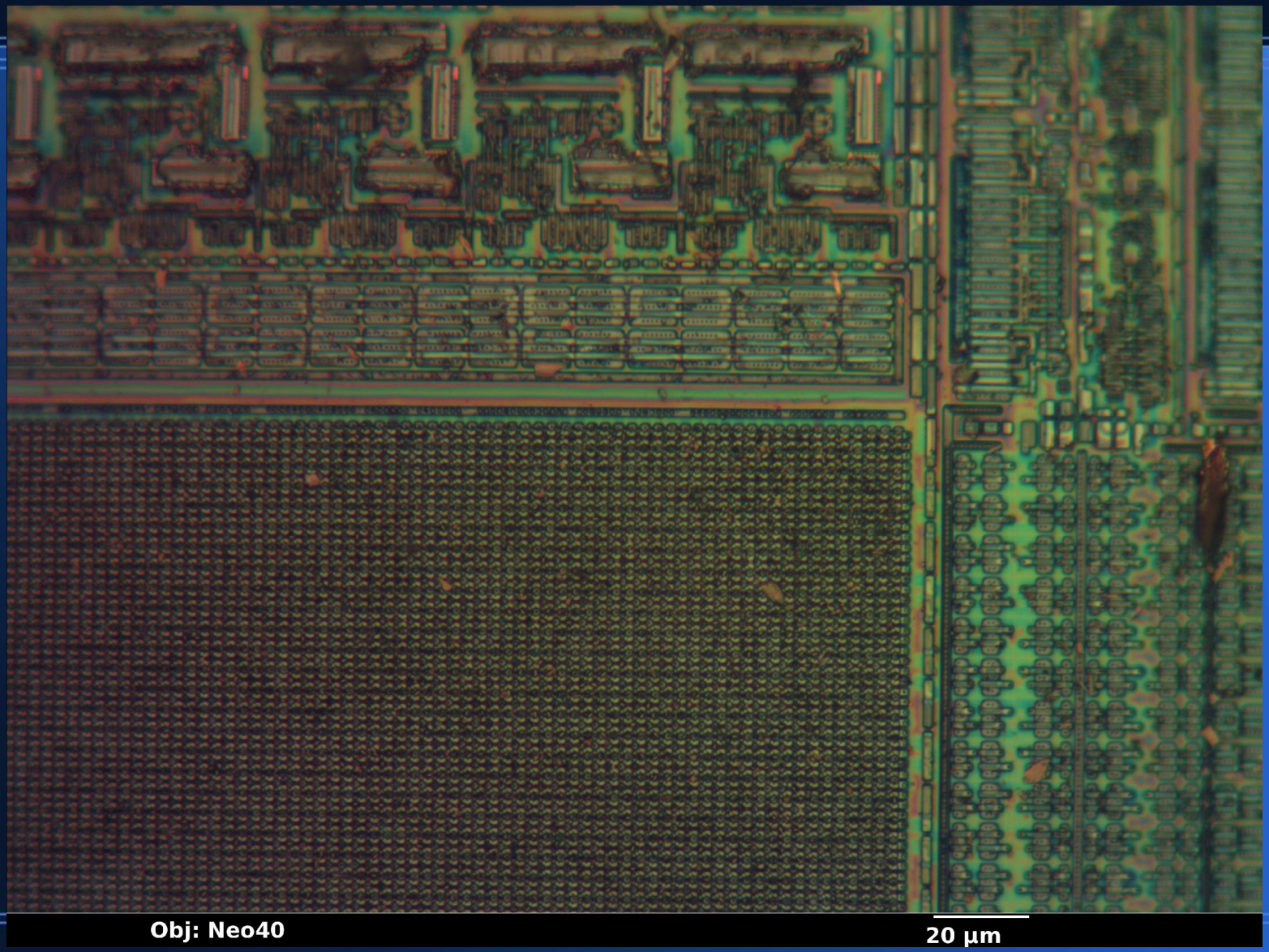




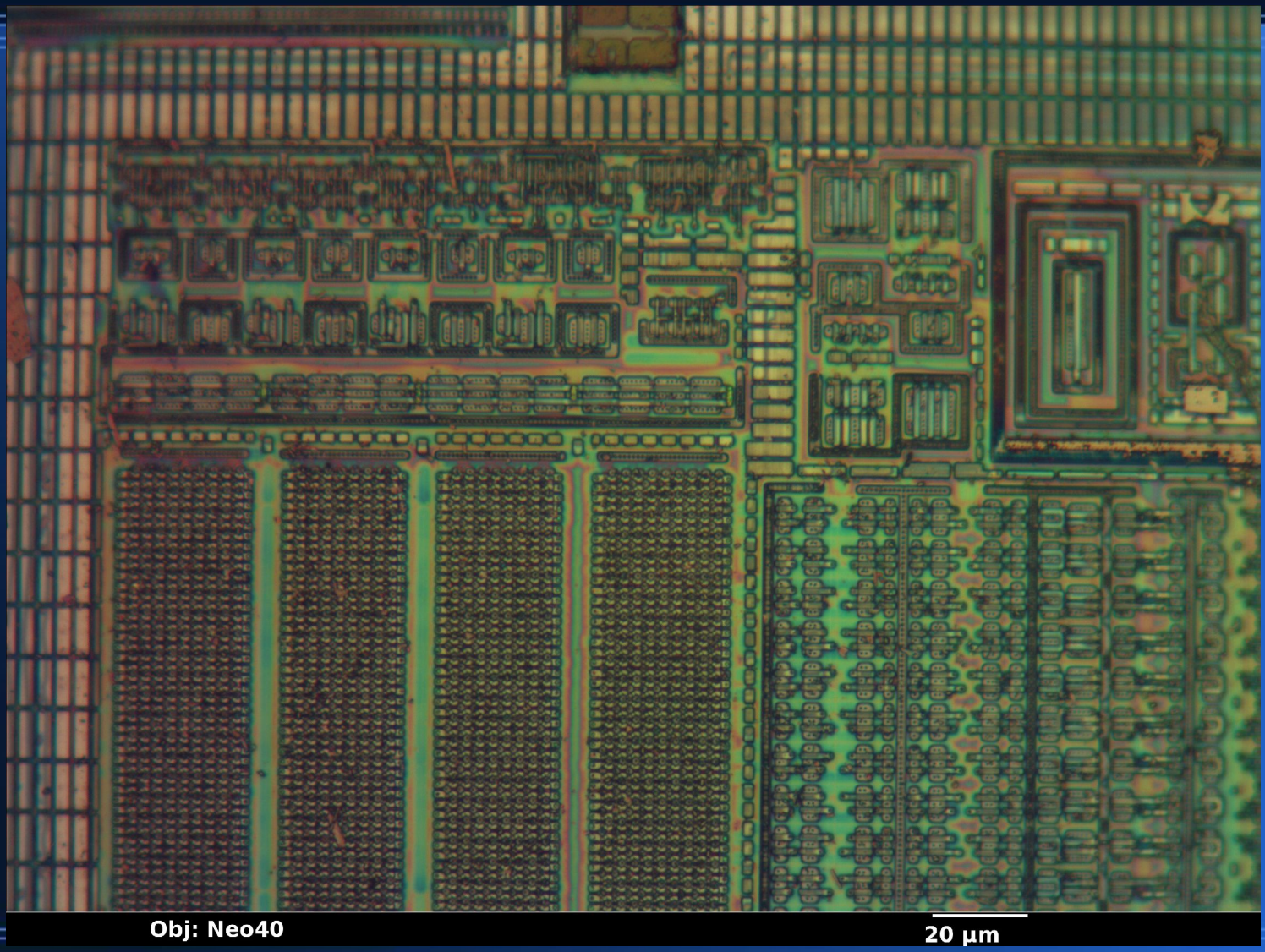
SRAM



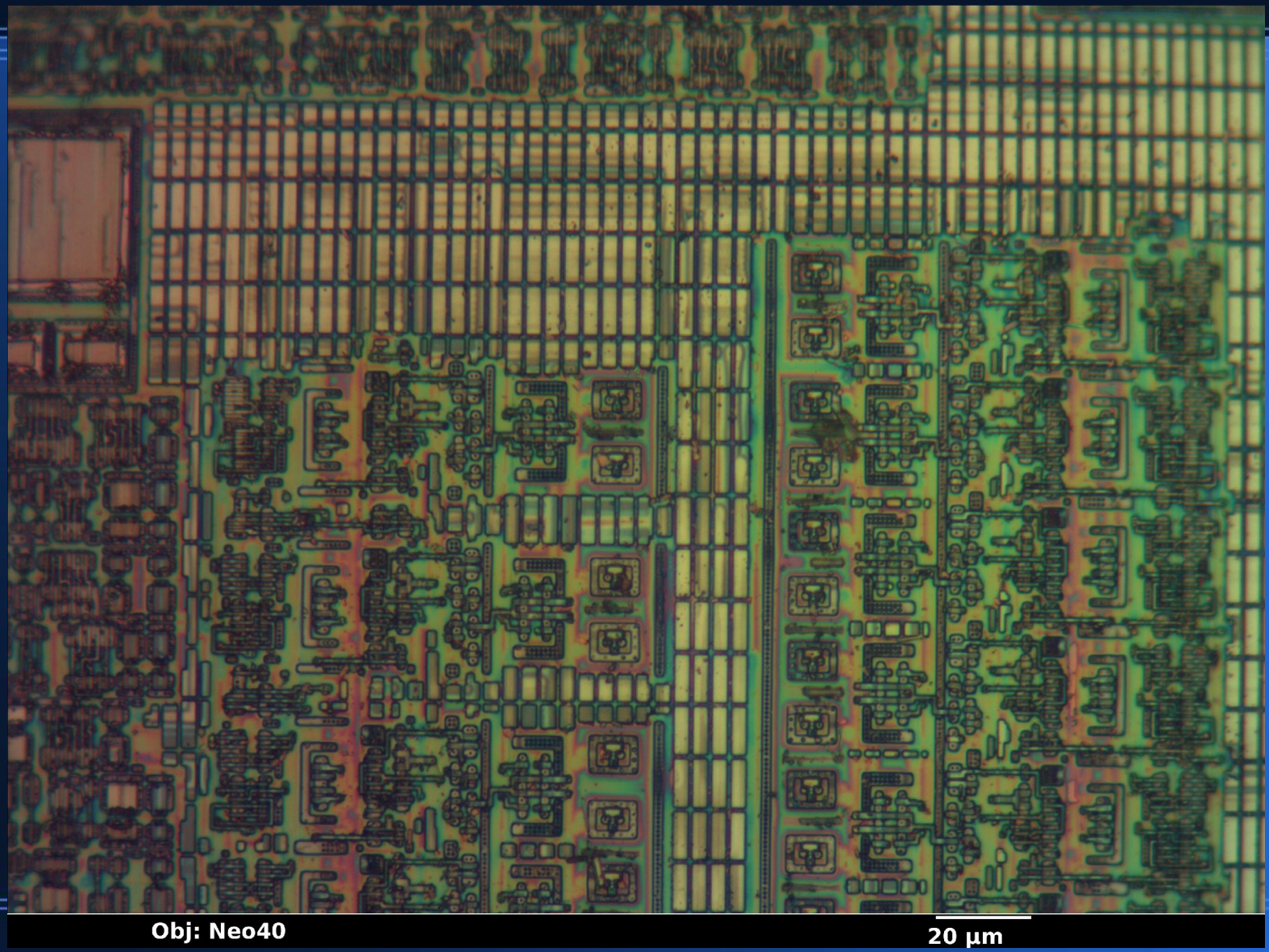
Flash



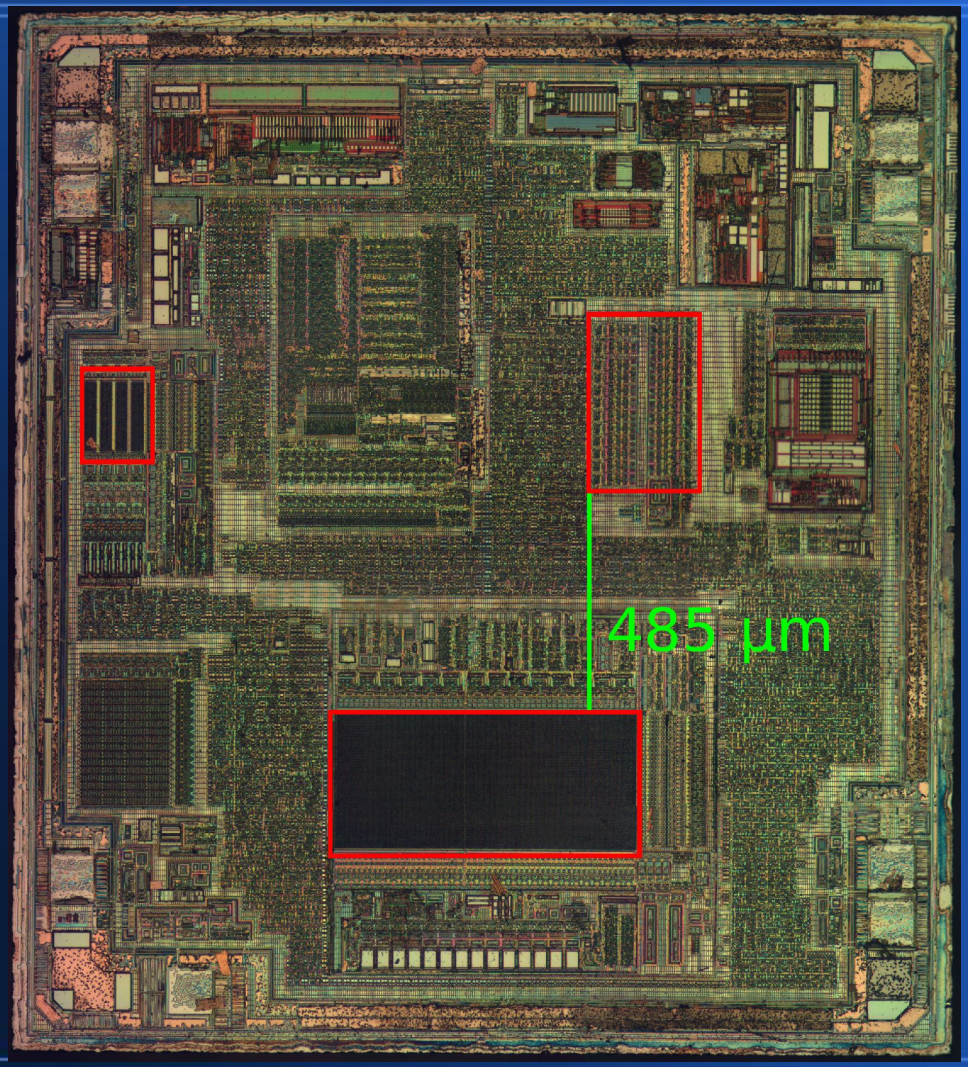
EEPROM



Config register

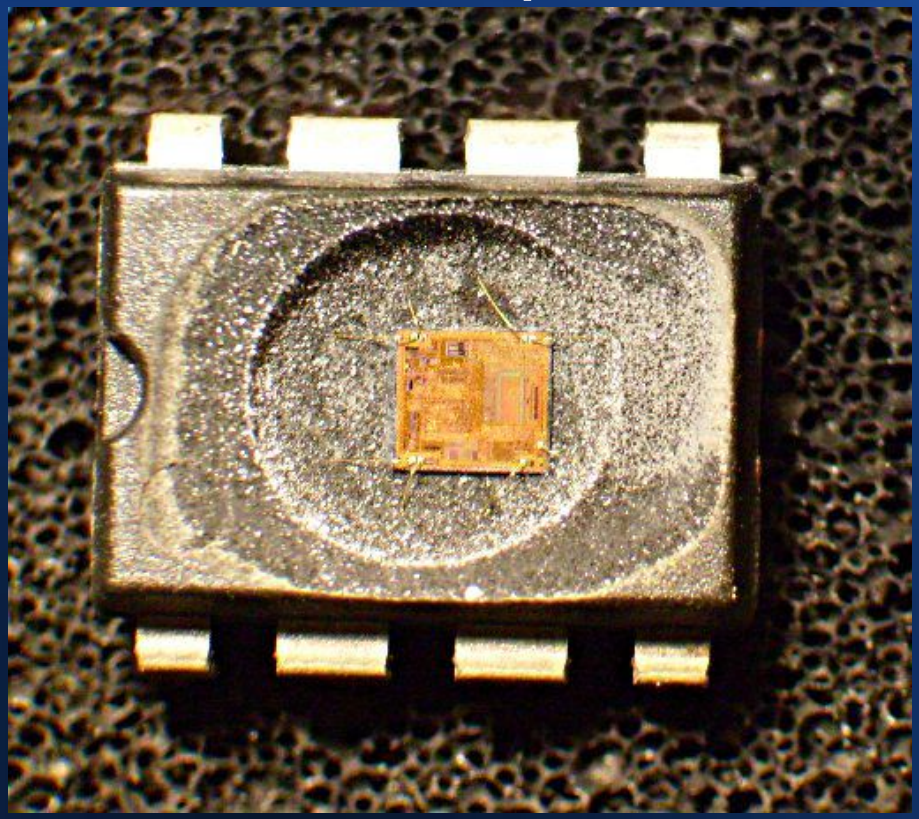


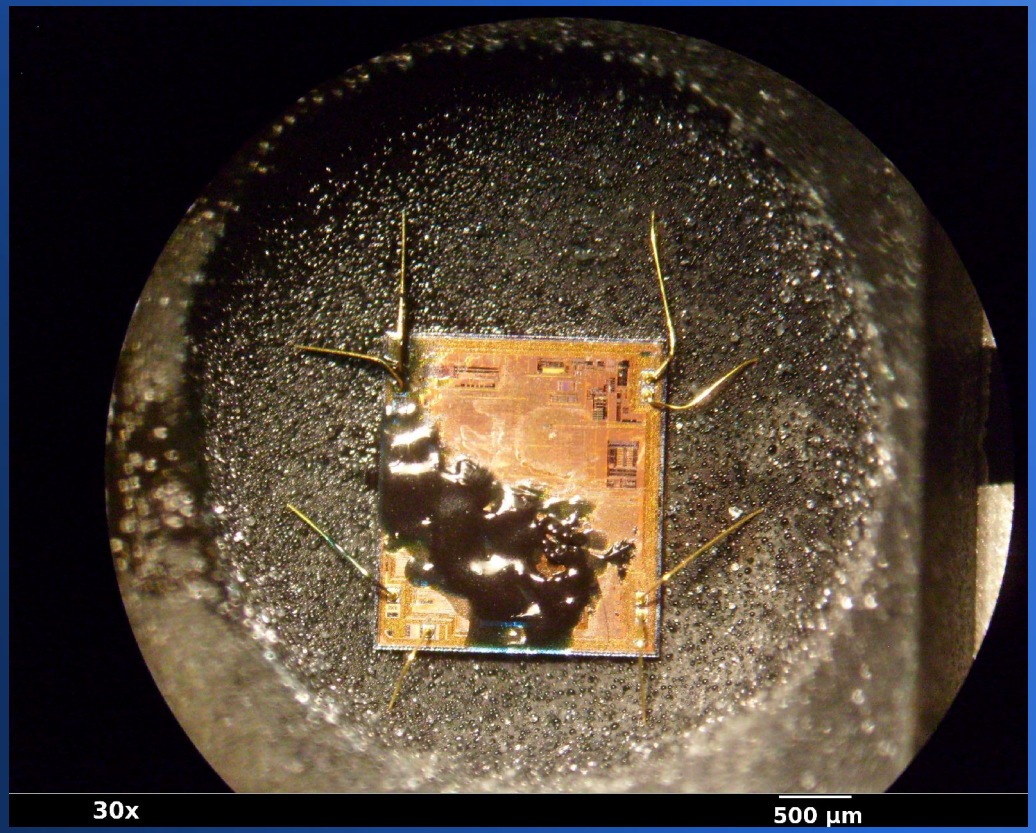
Memory array spacings



UV attack demo, part 1

- Black nail polish mask over die





UV attack demo, part 1

- Program target chip, set CP#
- Demonstrate readback failure
- Put in UV box and turn on

Optical fault injection

- Hook a laser or camera flash up to microscope
- Use aperture to focus light onto target area
- Apply precisely timed pulses to flip bits etc
  - Skorobogatov et al

Laser-assisted power analysis

- Similar setup to fault injection
- Apply weak laser beam to one half of a complementary pair
- If transistor is already on, nothing happens
- If transistor is off, it turns partially on
  - Increased leakage shows up in power trace

Invasive attacks

- Microprobing
- Circuit edits
  - Laser
  - FIB
- Other

Microprobing

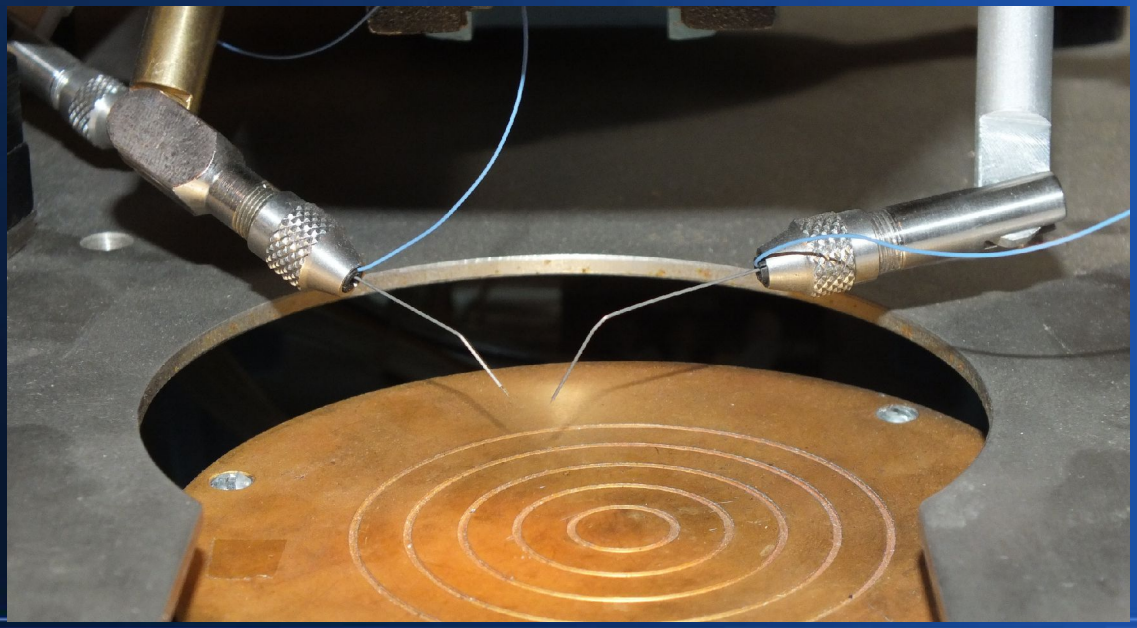
- Touch a conductive needle to a wire
- Connect probe to oscilloscope
  - May need pre-amplifier for weak/fast signals due to capacitive loading
- Hitting fine-pitch signals, or those not on top metal, may require more prep work

Microprobe stations

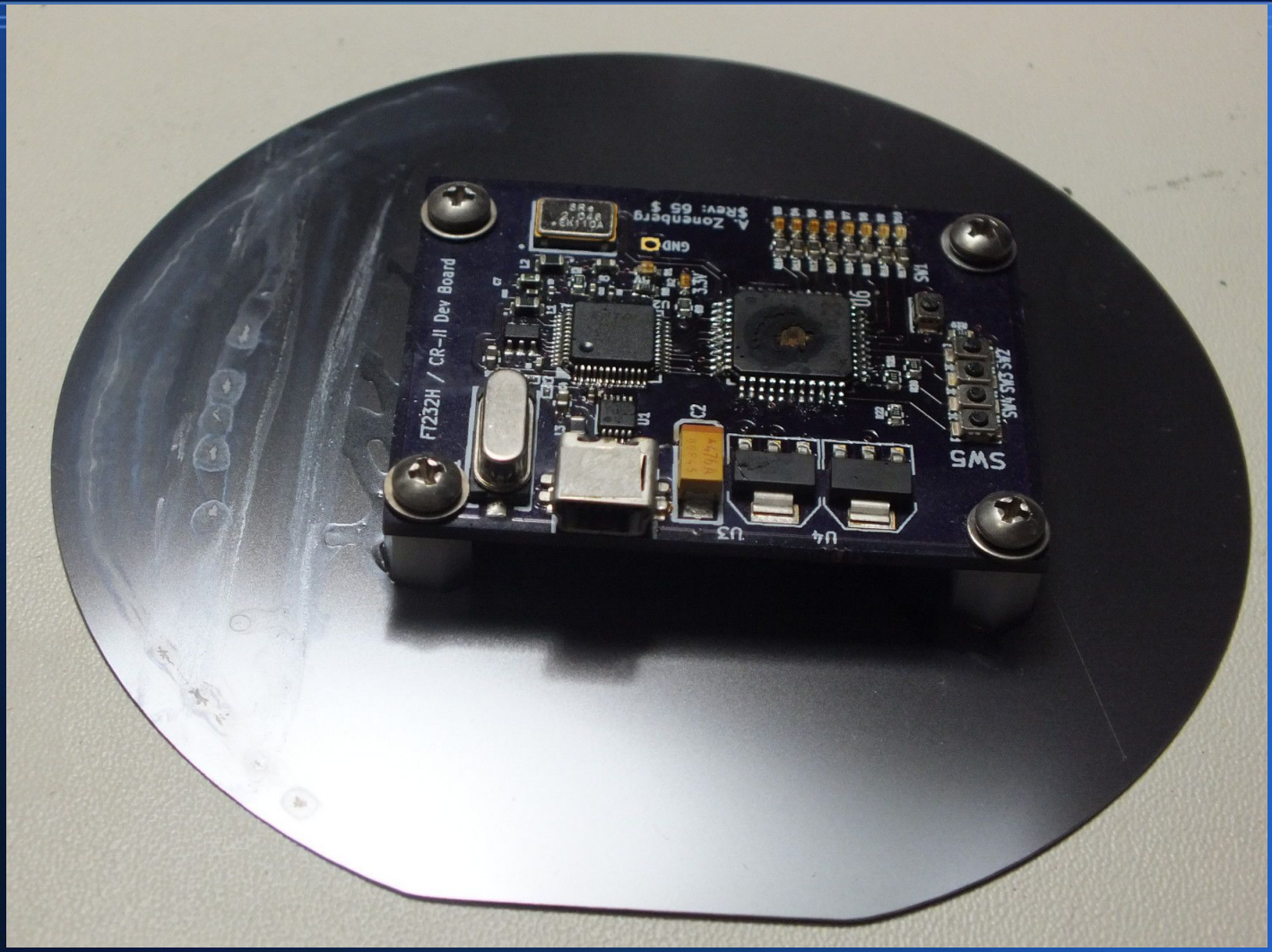
- Optical microscope w/ LWD obj
- Chuck for mounting sample
- Micropositioners

Sample mounting

- Some tweaking usually necessary
- Standard vacuum chucks fit full wafers
- May need custom jig for board/die



Sample mounting



Microprobes

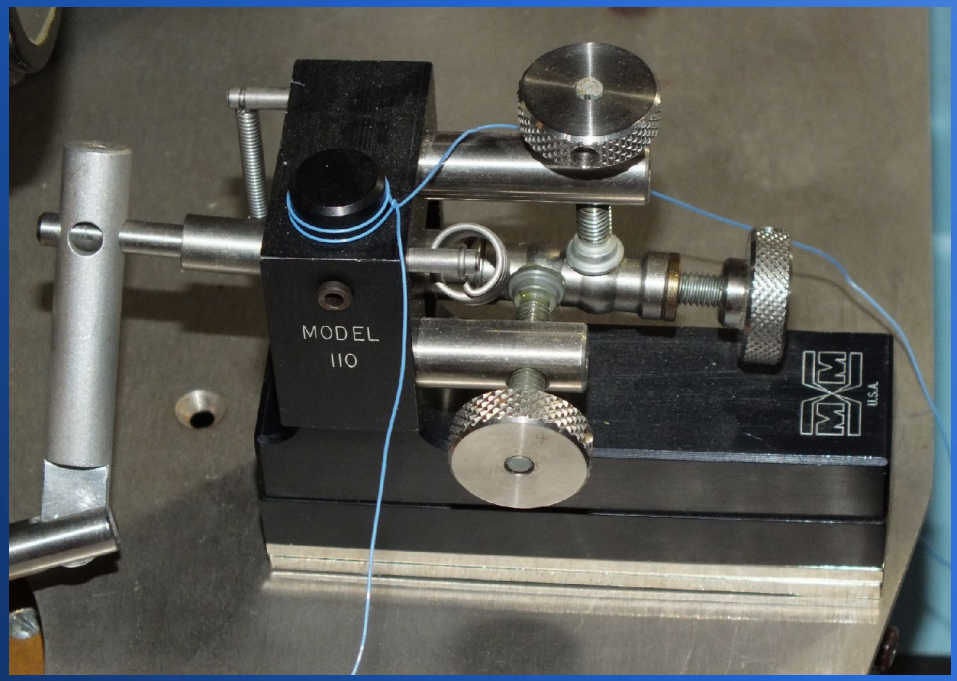
- Tungsten (usually) needle electrochemically sharpened to a fine point

Micropositioners

- Probe needle holder
- Reduction mechanism
- Base (vacuum or magnet)
- Quality is important!
  - Horrible backlash on my cheap ones

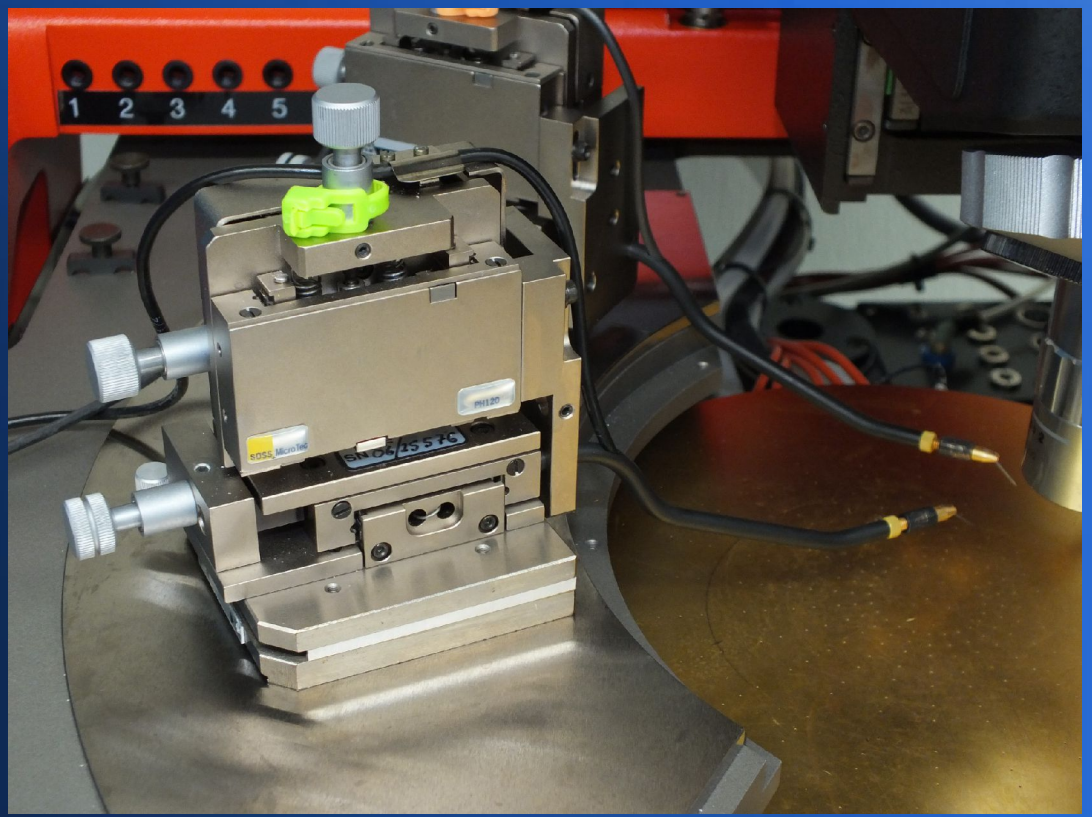
Polar micropositioner

- Lower cost
- Harder to use
- Single ball joint
  - Two tilt axes
  - One extension axis



Cartesian micropositioner

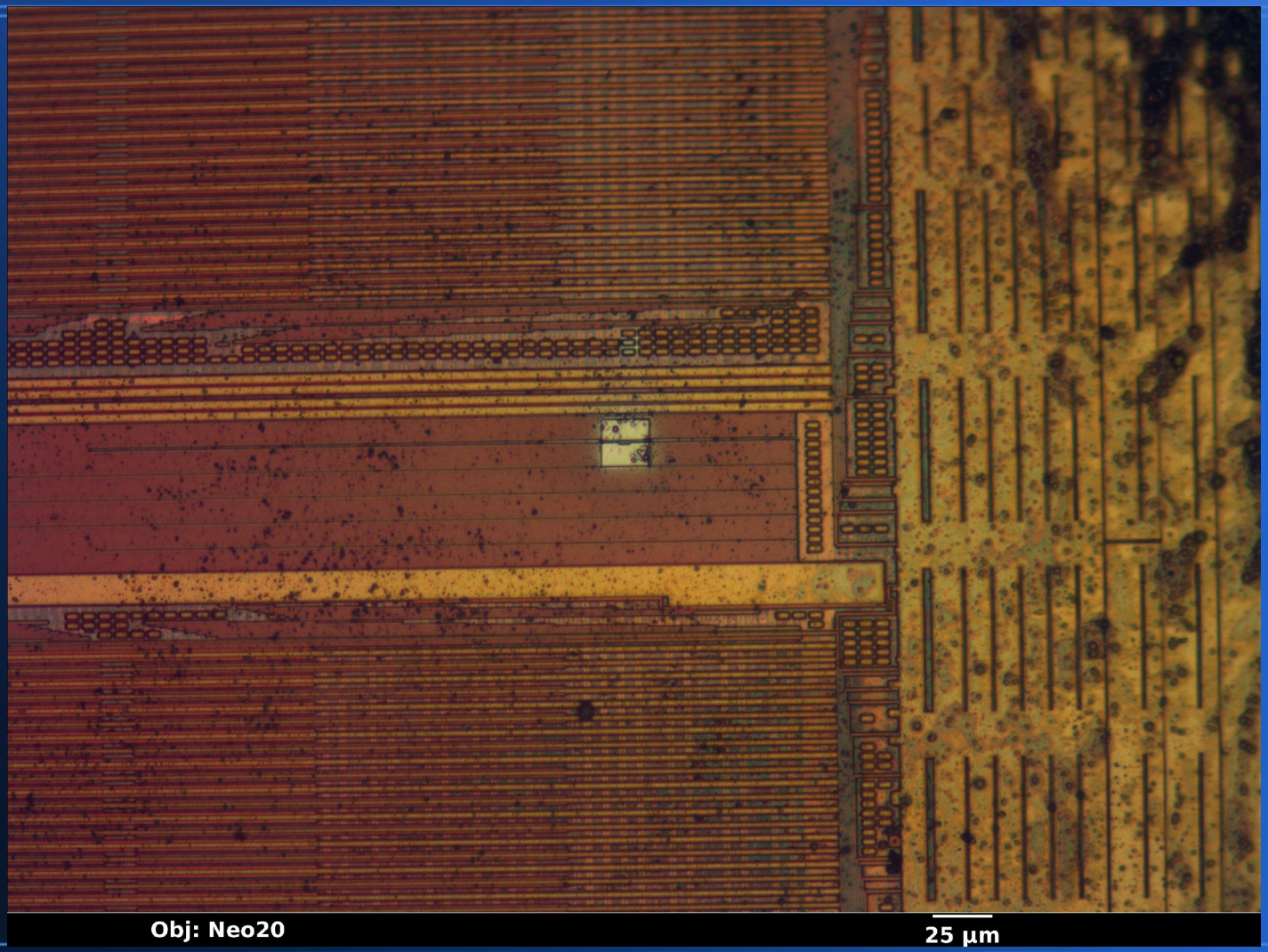
- Three linear stages at right angles
- More expensive
- Easier to use



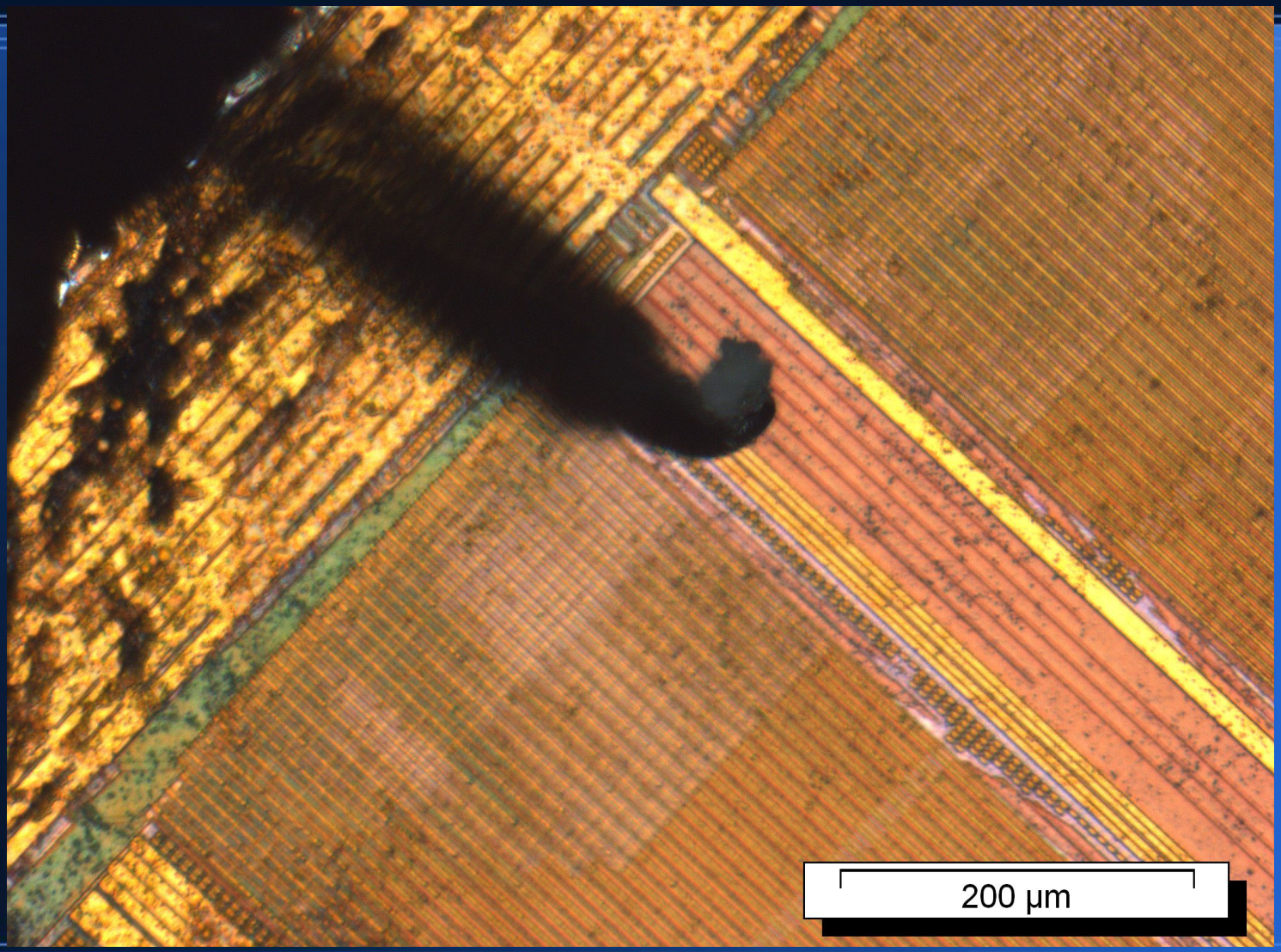
Microprobing

- Land probe needle on wire/pad and read stuff
- Landing too hard will damage pad/probe
- Look for slight sideways “scrub” motion on impact

Microprobing



Microprobing



Circuit edits

- Modify the target device in some way
- Destroy wires or transistors
- Add new wires
- Generally not practical to add new transistors

Laser cutting

- Specialized trinocular microscope
  - Mount laser instead of camera on top
- Several possible wavelengths
  - UV, green, IR most common
  - Choice depends on target material
- Shine beam through rectangular aperture

Laser cutting

- Fire short high-intensity pulses
  - CW will heat surrounding area
  - Pulses cause surface ablation
- Repeat until desired material is removed

Laser CVD

- Place sample in vacuum chamber
- Fill with low-pressure organometallic gas
  - $W(CO)_6$ is common tungsten precursor
- Gas adsorbs onto surface of die
- Low-energy laser pulses induce decomposition
  - Gaseous CO is released
  - Solid W stays on surface

Laser CVD

- Use multiple laser shots to increase thickness
- Adjusting beam shape and scanning across surface allows deposition area to be controlled
- Limited resolution
  - Optical diffraction
  - Heat transfer through material

Focused ion beam (FIB)

- Similar to SEM
  - Uses ionized atoms instead of electrons
- Liquid-metal ion source (LMIS)
  - Tungsten tip similar to field-emission gun
  - Wet tip with liquid Ga
  - Extraction voltage pulls Ga+ ions off tip

Theory of FIB operation

- Ion beam can be manipulated like an e-beam
- Ions emit secondary electrons at impact point
  - Can be used for imaging like SEM
- But kinetic energy of Ga+ is >> that of e-
  - Causes sputtering at point of impact
  - Damages surface
  - Can image with secondary ions
  - Spectroscopy possible too (SIMS)

Dual-beam SEM/FIB

- Two columns on one vacuum chamber
  - Electron gun for imaging
  - Ion gun for milling
- Single set of detectors
- Mix and match both beams
- RPI has two!
  - Zeiss 1540 in cleanroom
  - FEI Versa in MRC (brand new)

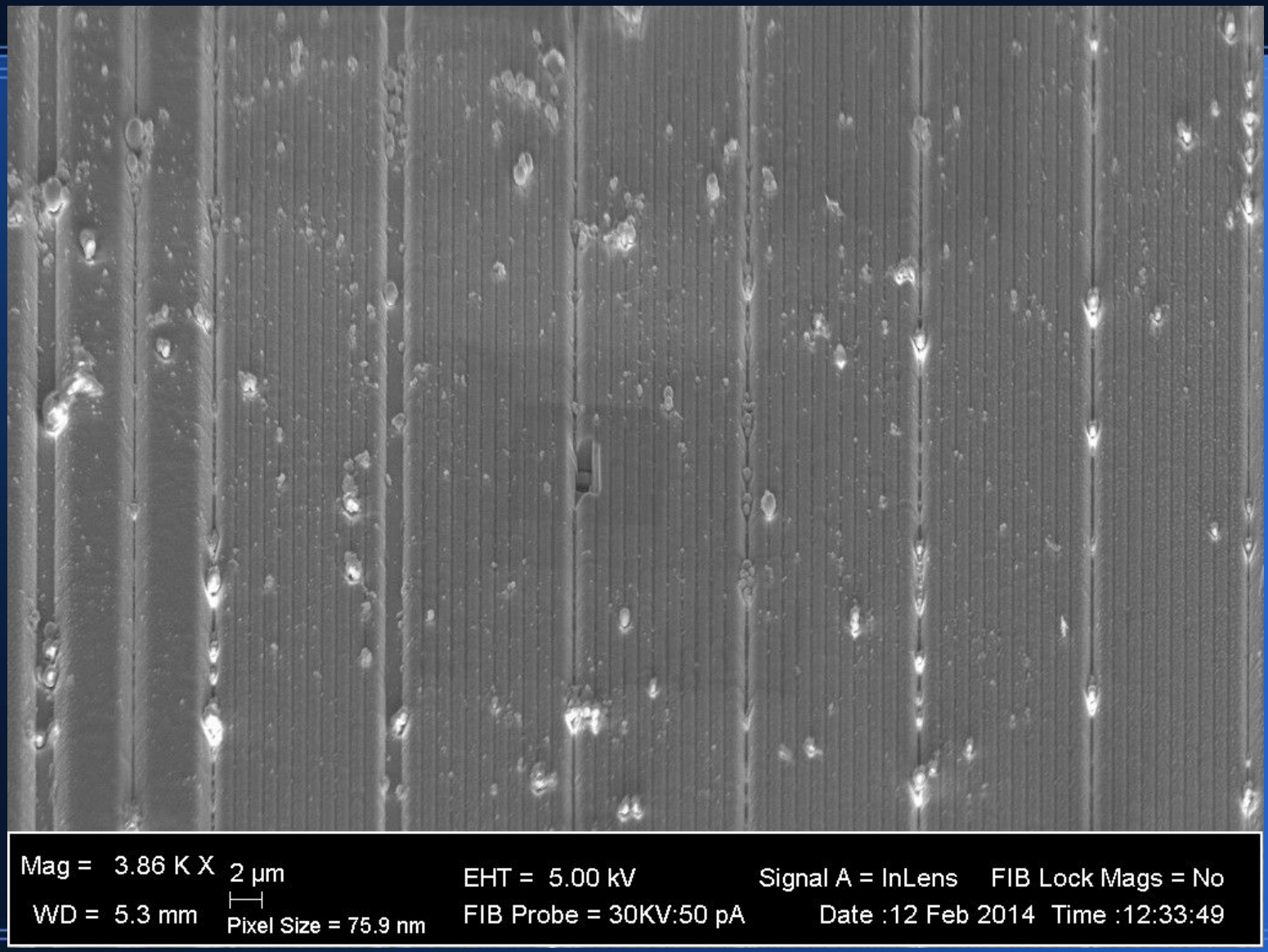
FEI Versa 3D

Close quarters in chamber

FIB milling

- Use ion beam at high current
  - Beam will sputter anything it hits
  - Scan across region to be cut
- Not perfect cuts
  - Some Ga+ is implanted in the face of the cut
  - Sputtered material may deposit around the cut

FIB milling


Mag = 3.86 K X
2 µm
WD = 5.3 mm
Pixel Size = 75.9 nm
EHT = 5.00 kV
FIB Probe = 30KV:50 pA
Signal A = InLens
FIB Lock Mags = No
Date :12 Feb 2014 Time :12:33:49

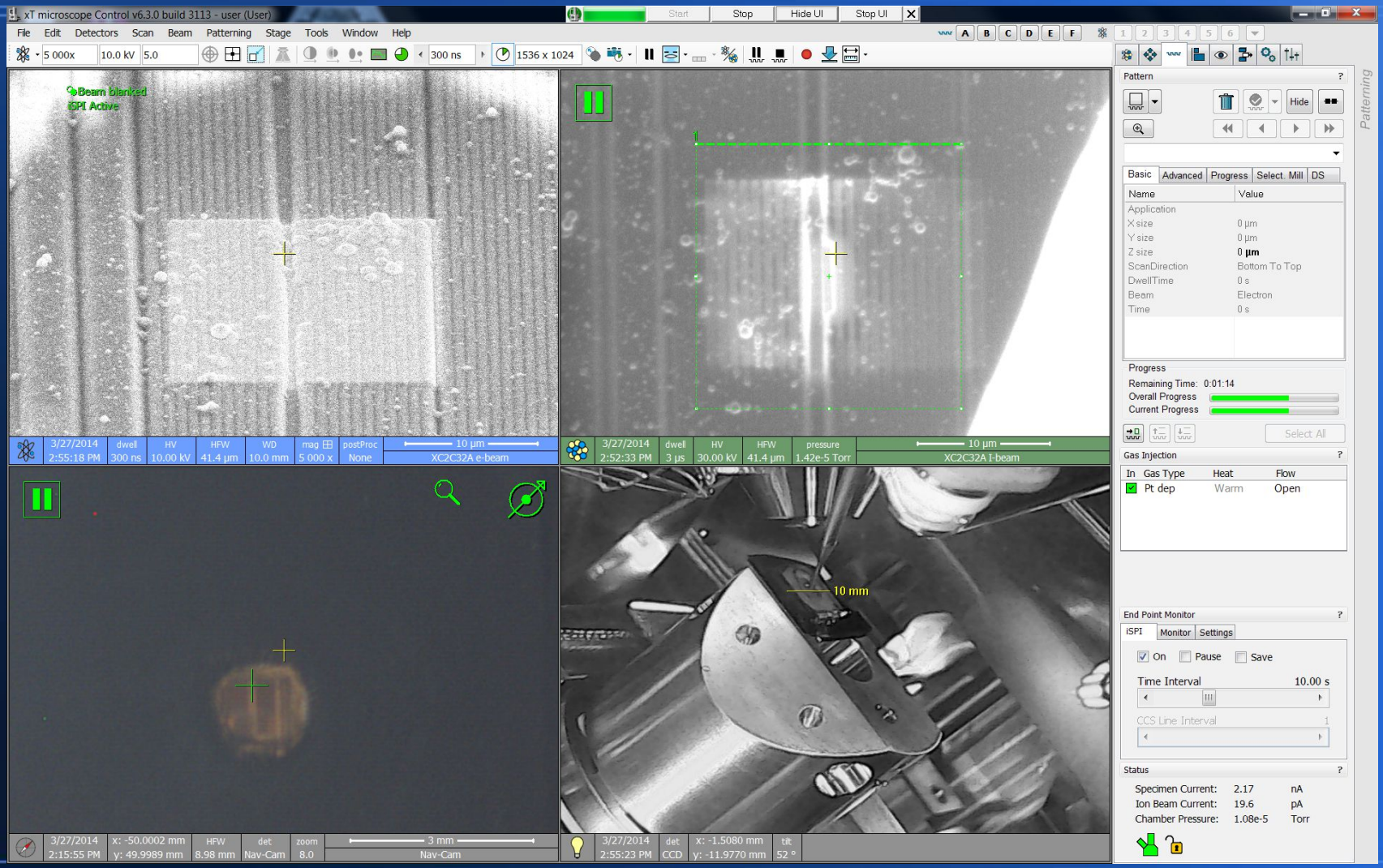
FIB CVD

- Very similar to laser CVD
- Inject precursor gas into chamber
- Scan ion beam or e-beam over target region
- Secondary electrons induce decomposition
  - SE interaction volume can be large
  - Some “overspray” may occur
  - Use final low-current mill to clean up

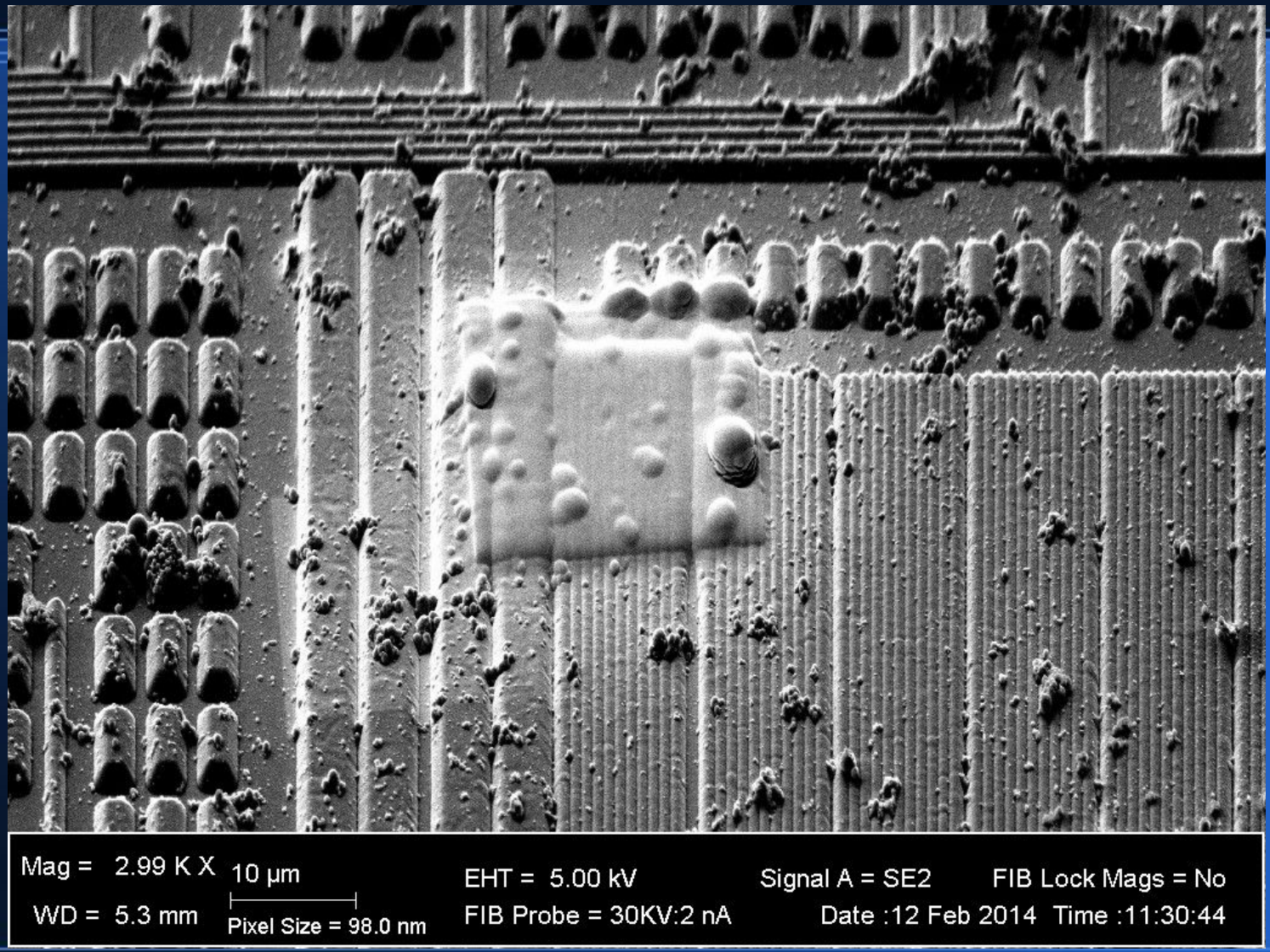
FIB CVD

- Video
  - https://www.youtube.com/watch?v=Z2JWaImre64

FIB CVD


xT microscope Control v6.3.0 build 3113 - user (User)
Start
Stop
Hide UI
Stop UI
File
Edit
Detectors
Scan
Beam
Patterning
Stage
Tools
Window
Help
Beam blanked
iSPI Active
10 µm
XC2C32A e-beam
XC2C32A I-beam
10 mm
3 mm
Nav-Cam
Pattern
Hide
Basic
Advanced
Progress
Select Mill
DS
Name
Value
Application
X size
Y size
Z size
ScanDirection
Bottom To Top
DwellTime
Beam
Electron
Time
Progress
Remaining Time: 0:01:14
Overall Progress
Current Progress
Select All
Gas Injection
In
Gas Type
Heat
Flow
Pt dep
Warm
Open
End Point Monitor
iSPI
Monitor
Settings
On
Pause
Save
Time Interval
10.00 s
CCS Line Interval
Status
Specimen Current: 2.17 nA
Ion Beam Current: 19.6 pA
Chamber Pressure: 1.08e-5 Torr
Patterning

FIB CVD


Mag = 2.99 K X
10 µm
WD = 5.3 mm
Pixel Size = 98.0 nm
EHT = 5.00 kV
FIB Probe = 30KV:2 nA
Signal A = SE2
FIB Lock Mags = No
Date :12 Feb 2014 Time :11:30:44

Other circuit edit techniques

- Material removal
  - Lithography: Coat photoresist, expose with epi-illuminator or similar, develop, wet etch
- Material deposition
  - Cut holes over interesting nets
  - Evaporate/sputter whole die with conductive material
  - Lift-off or etch to pattern

UV attack demo, part 2

- Readout test

Questions?

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