IC Reverse Engineering

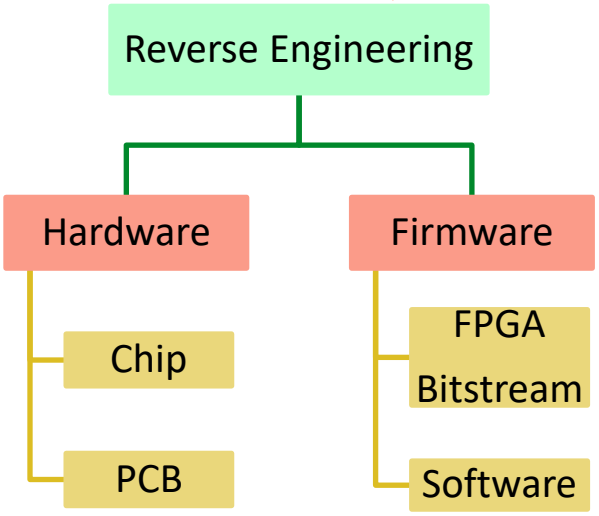
Navid Asadi

Physical Inspection and AttacKs on ElectronicS (PHIKS)

Reverse Engineering

Primary Purpose of RE

- ✓ Analyzing internal structure to extract netlist
- ✓ Extracting functionality or firmware



Chip Level RE

- ✓ 5 Steps for complete chip RE

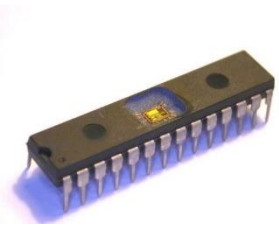
Imaging
- SEM/ Optical

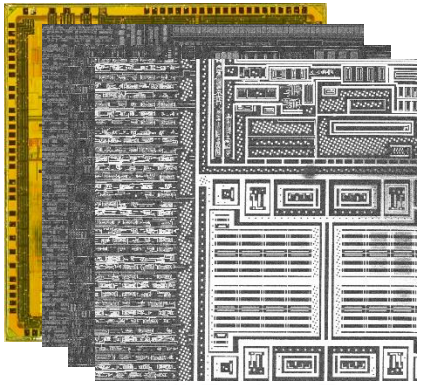
Depacakging
- Selective - Frontside
- Non-selective - Backside

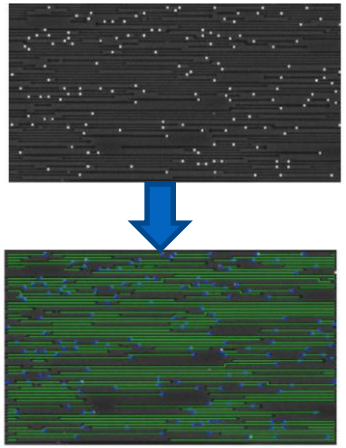
Delayering
- Plasma/FIB etching
- Wet etching

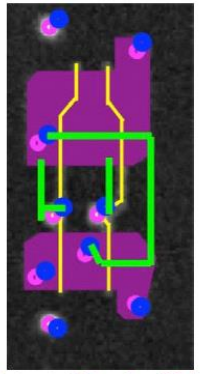
Annotation
- Extract Layer Information

Functionality
- Extract netlist
- VHDL code







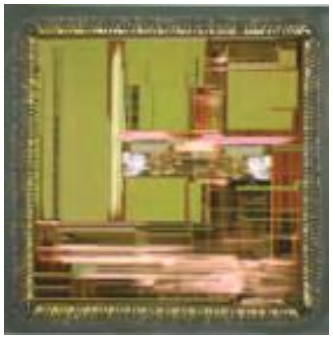


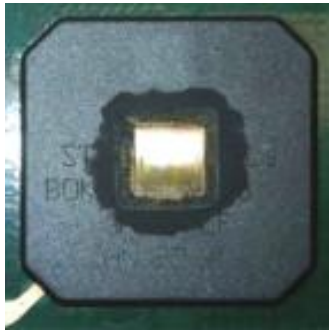
Extracted Standard Cells

FCS Research

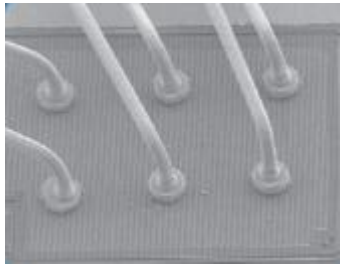
De-packing

- Acid etching
  - Temeprature control
  - Sulfuric acid
  - Nitric Acid
  - Mixed acid
  - Rinse acid





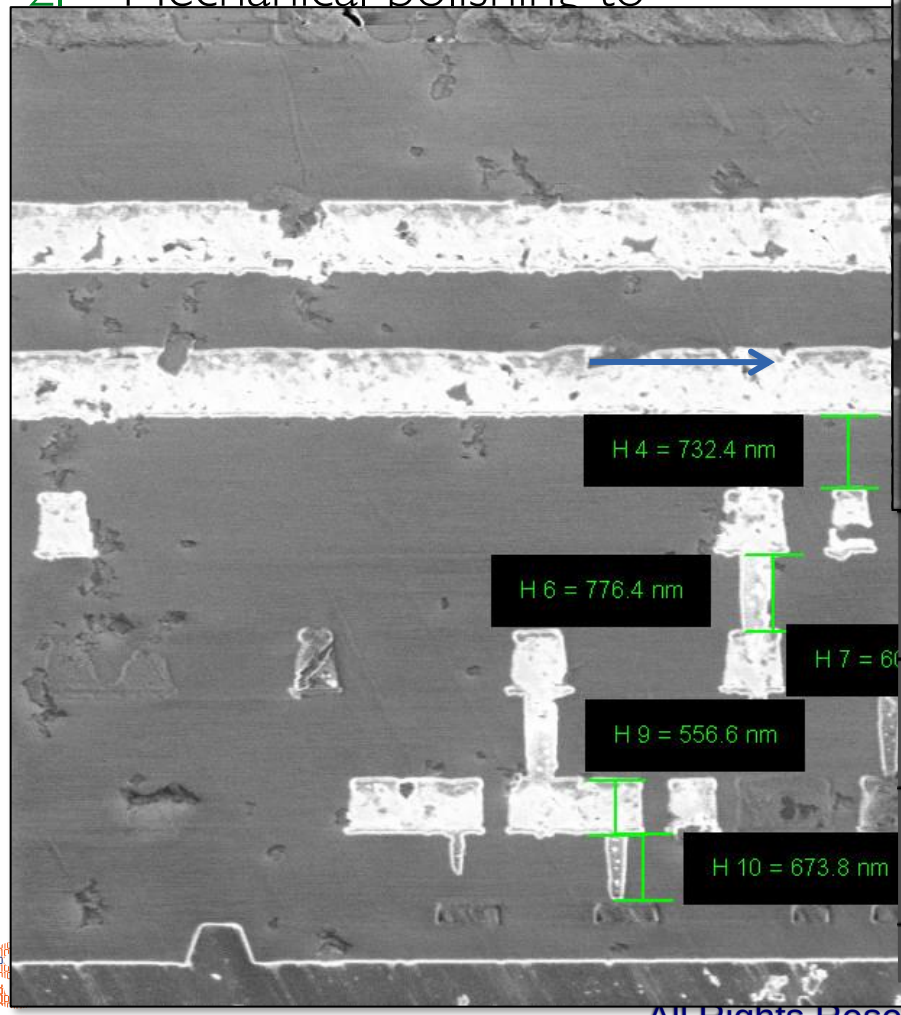
- Bond wire protect
  - Maintain integrity of sensitive components

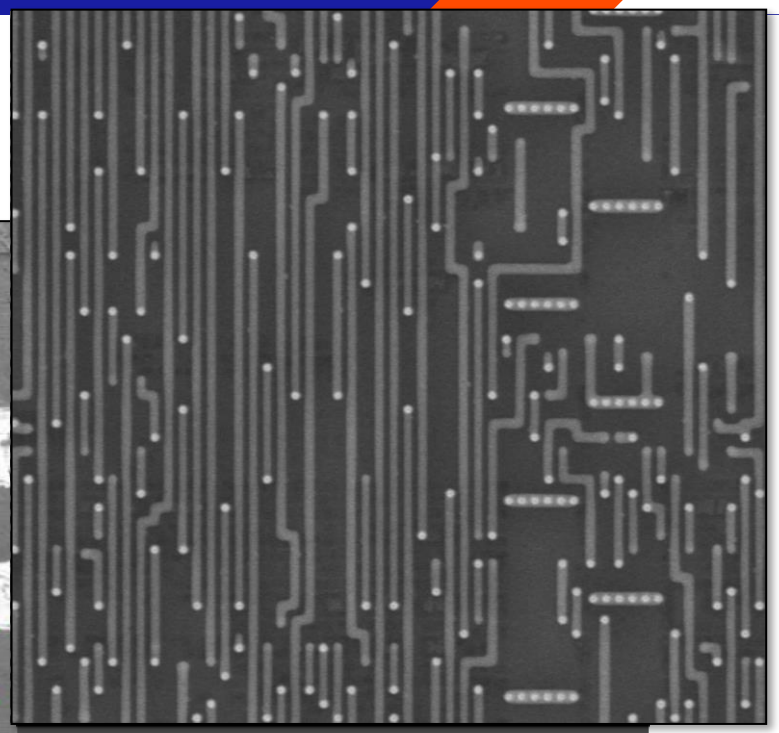


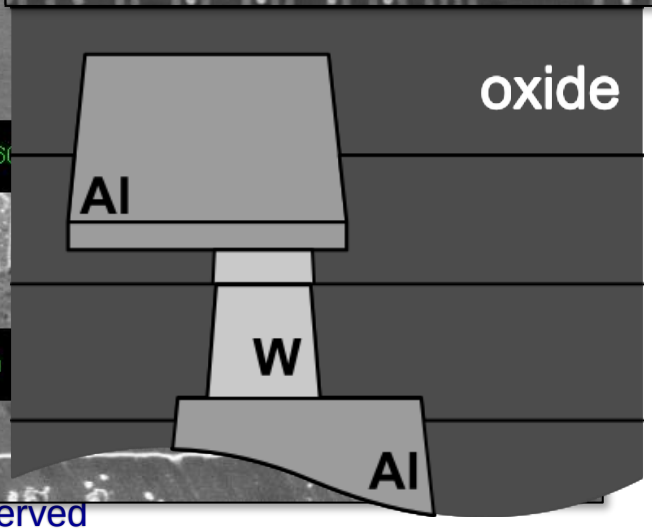
- Microwave induced plasma etching
  - Microwaved gas is inciting chemical radicals for isotropic etching
  - The gas mass flow controls the etching rate
  - Can protect silver or copper bod wires

Chip delayering. Methodology

- Delayering steps:
  1. Technological map
  2. Mechanical polishing to

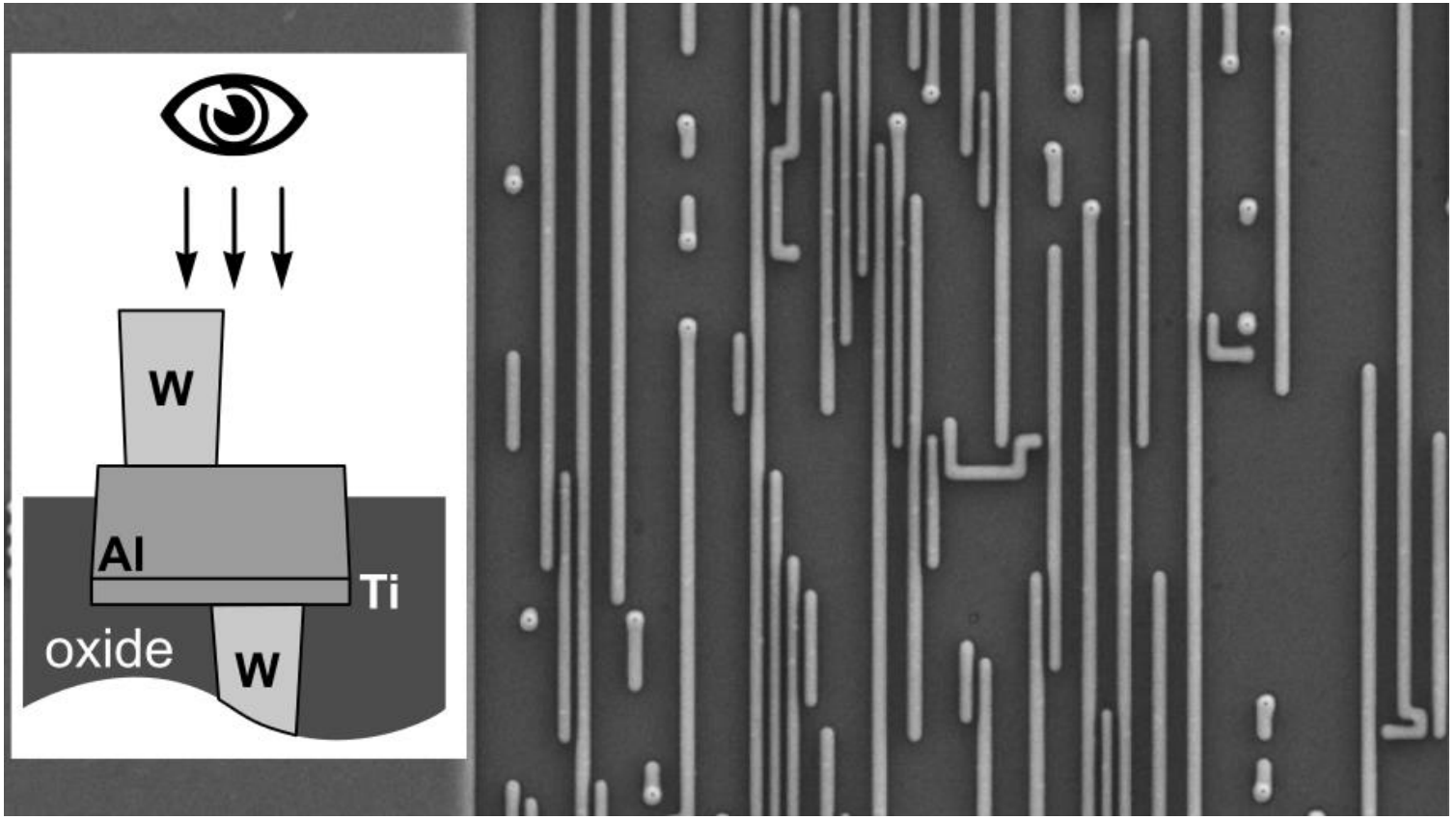






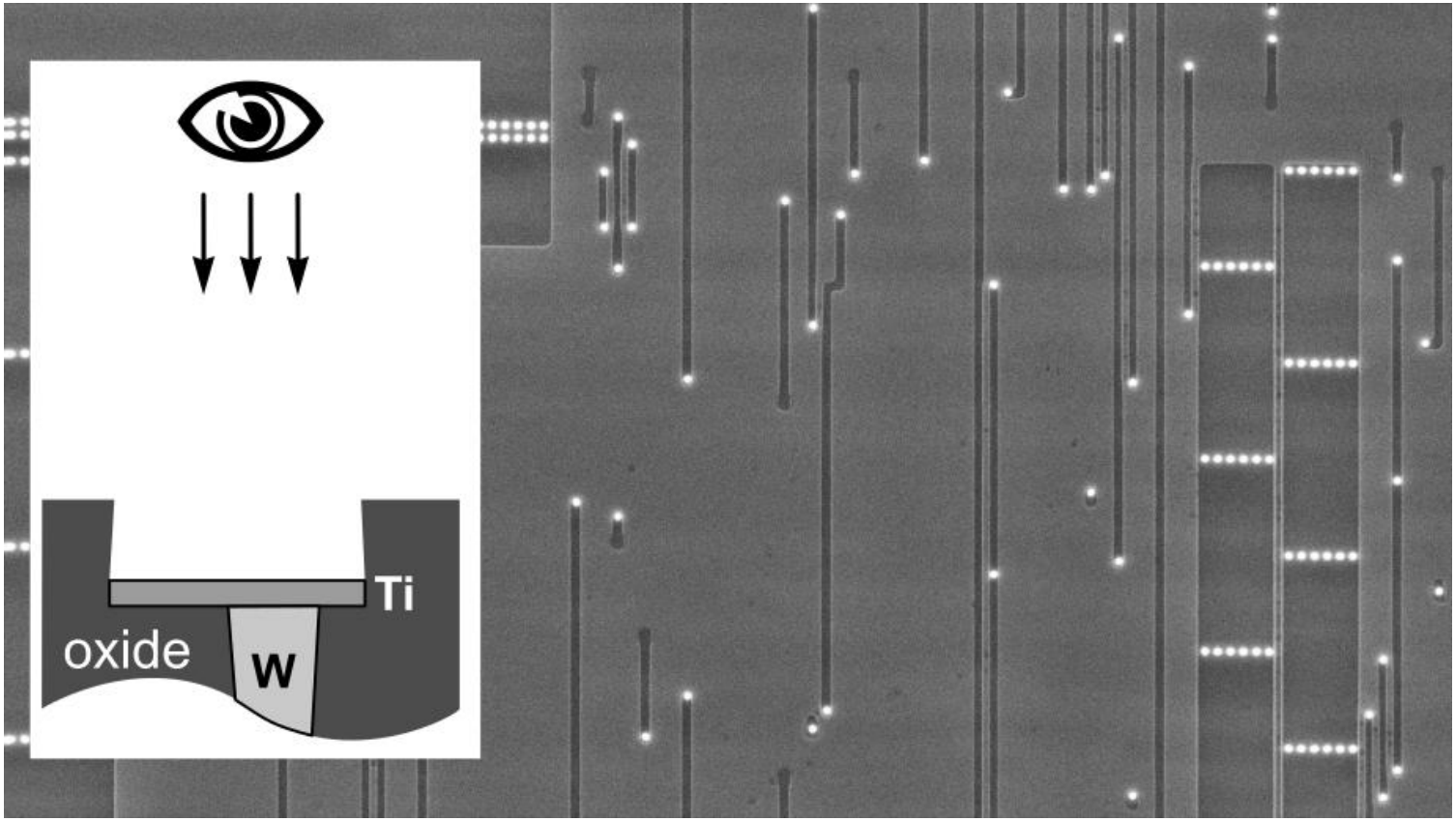
Chip delayering. Imaging Option A

- ✓ good SiO_2 margin
- ✓ easy via removing
- ✓ good image contrast
- ✗ bad mechanical stability



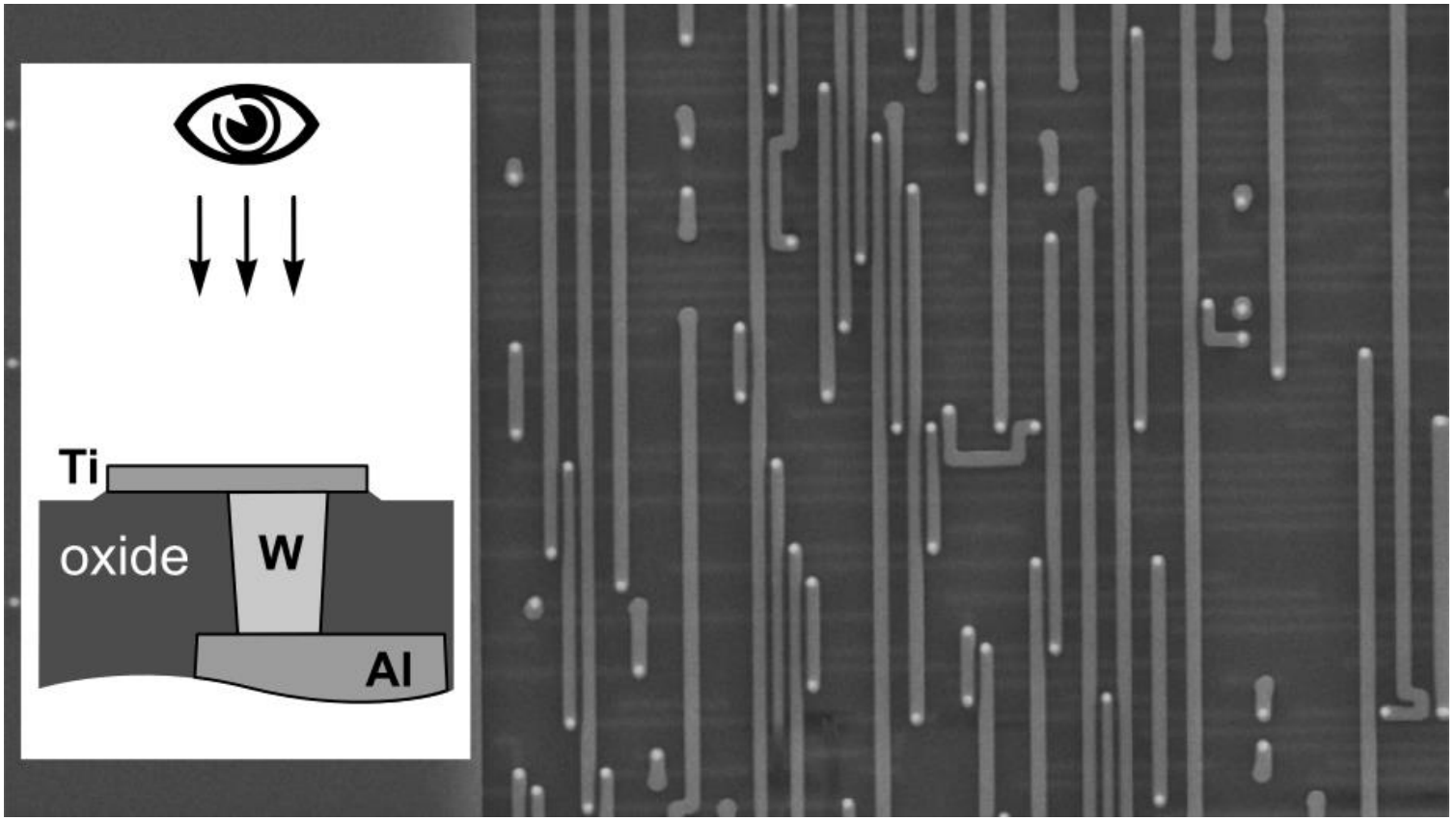
Chip delayering. Imaging Option B

- ✓ good SiO_2 margin
- ✓ ✓ great image contrast
- ✓ ✓ great mechanical stability
- ✘ ✘ critical via removing (not suitable for Cu based techs)



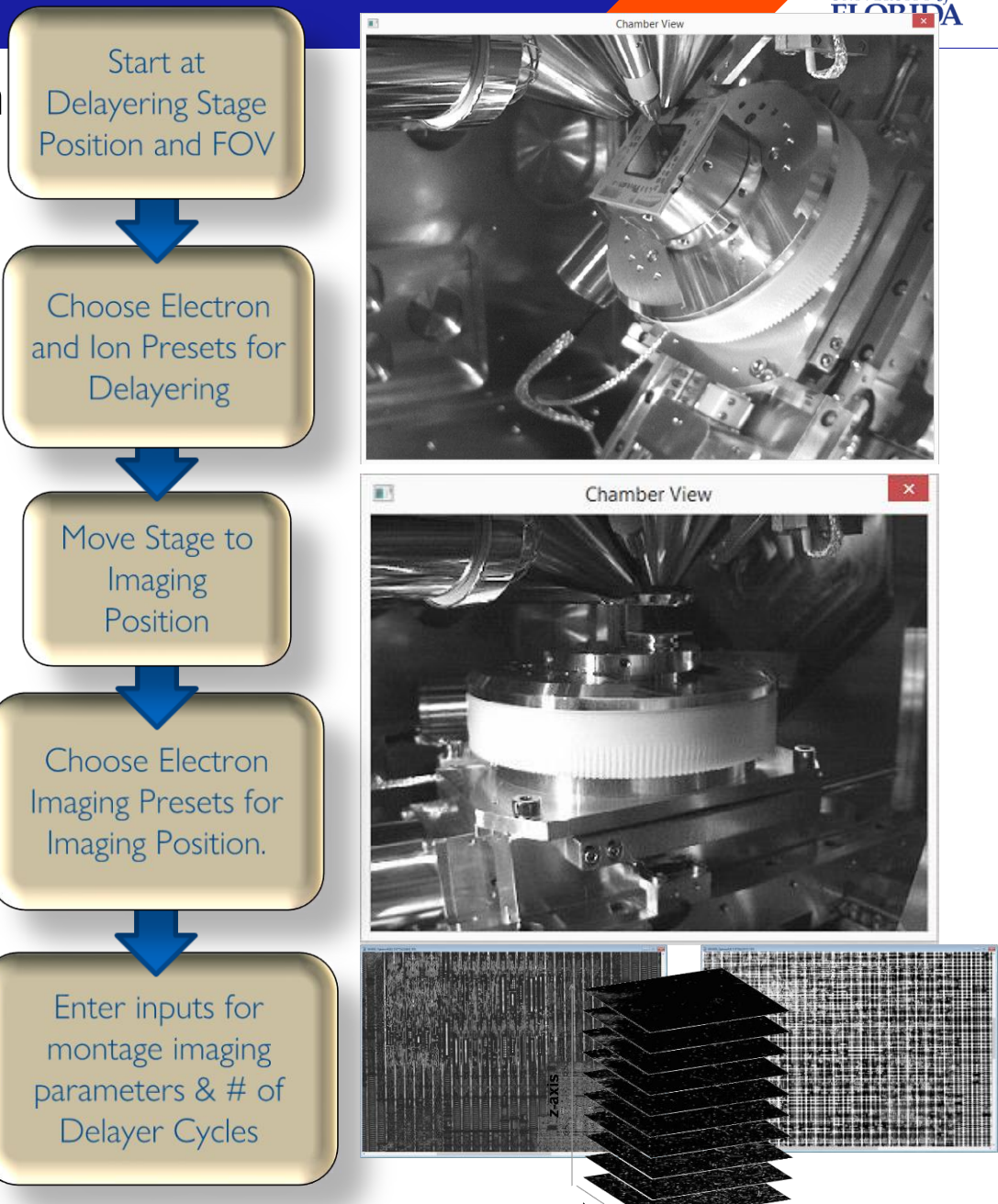
Chip delayering. Imaging Option C

- ✓ good mechanical stability
- ✓ easy via removing
- ✘ critical SiO_2 margin
- \- fair image contrast



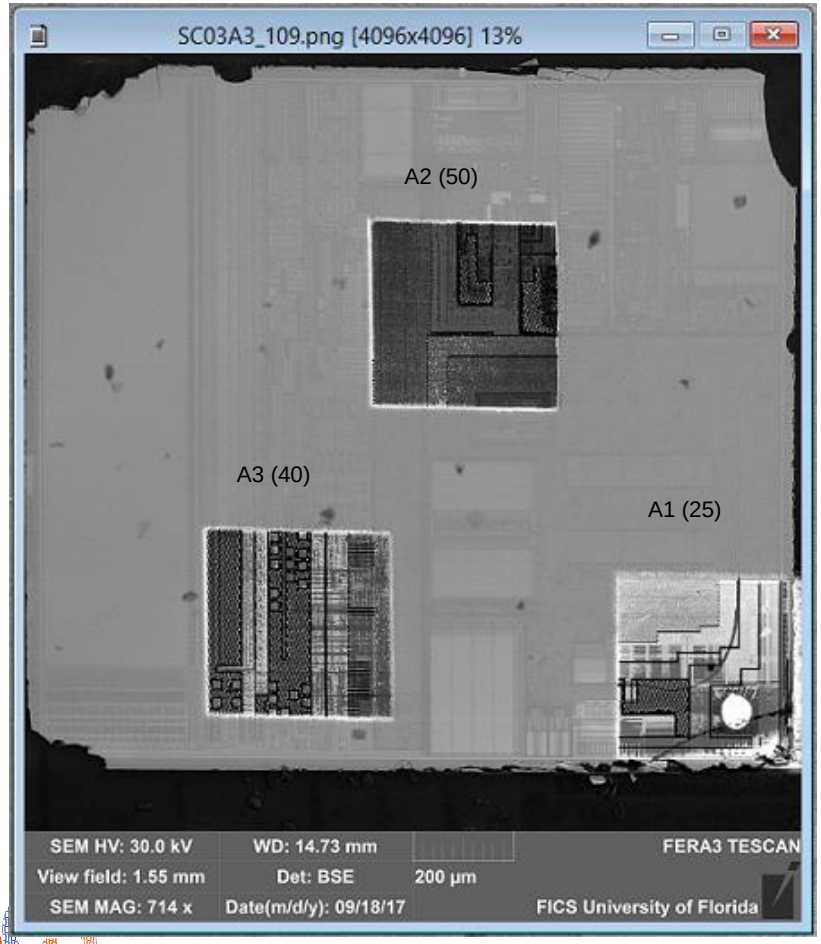
Auto Delayering Workflow

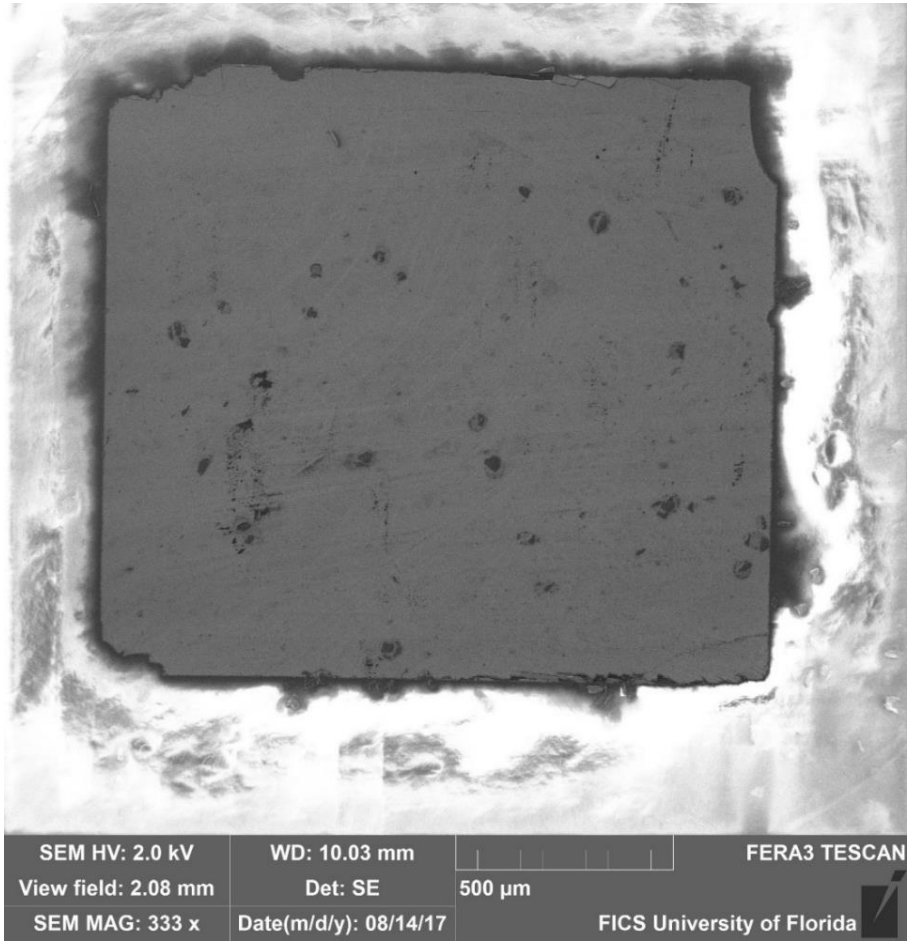
- User defined delayering position and FOV is read.
- Ion and electron presets are selected for delayering:
- Imaging stage position read:
  - Zero tilt
  - Below-the-lens BSE detector
- Multiple imaging voltages and detectors may be defined via presets.
- User-selected FOV, dwell time, pixel density & number of cycles.



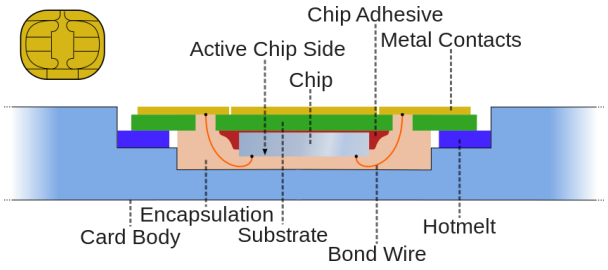
Case Study: Smartcard

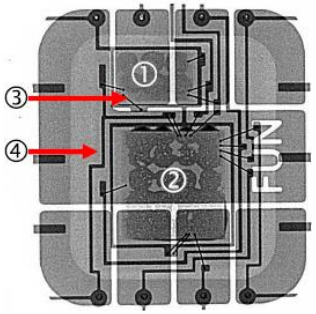
- Basic Card OS w/ 2k EEPROM/3DES Encryption
- Three Areas: A1, A2, A3 shown with number of automated layers in parentheses

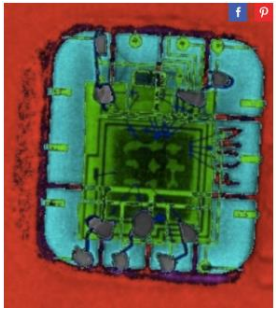




Chip Cards Vulnerability

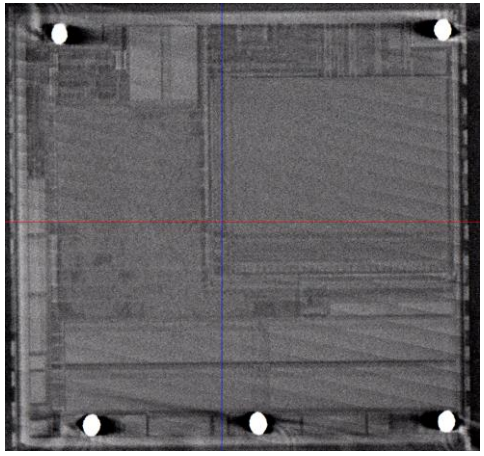




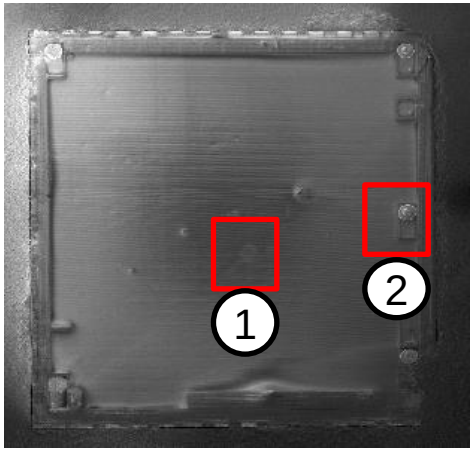


FUN chip added to the chip card
Allows to accept any PIN
$680,000 was stolen

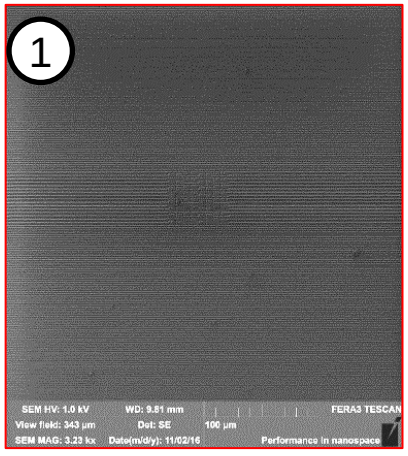
3D X-ray image
image resolution :0.7 um

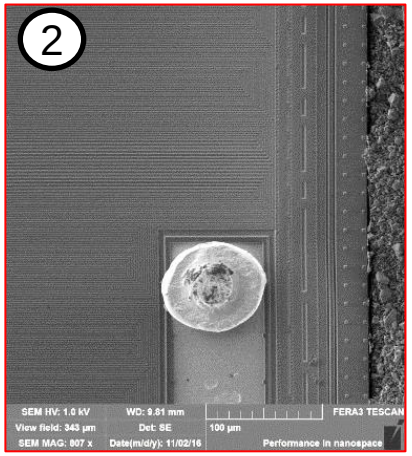


2D SEM image
image resolution: 10 nm



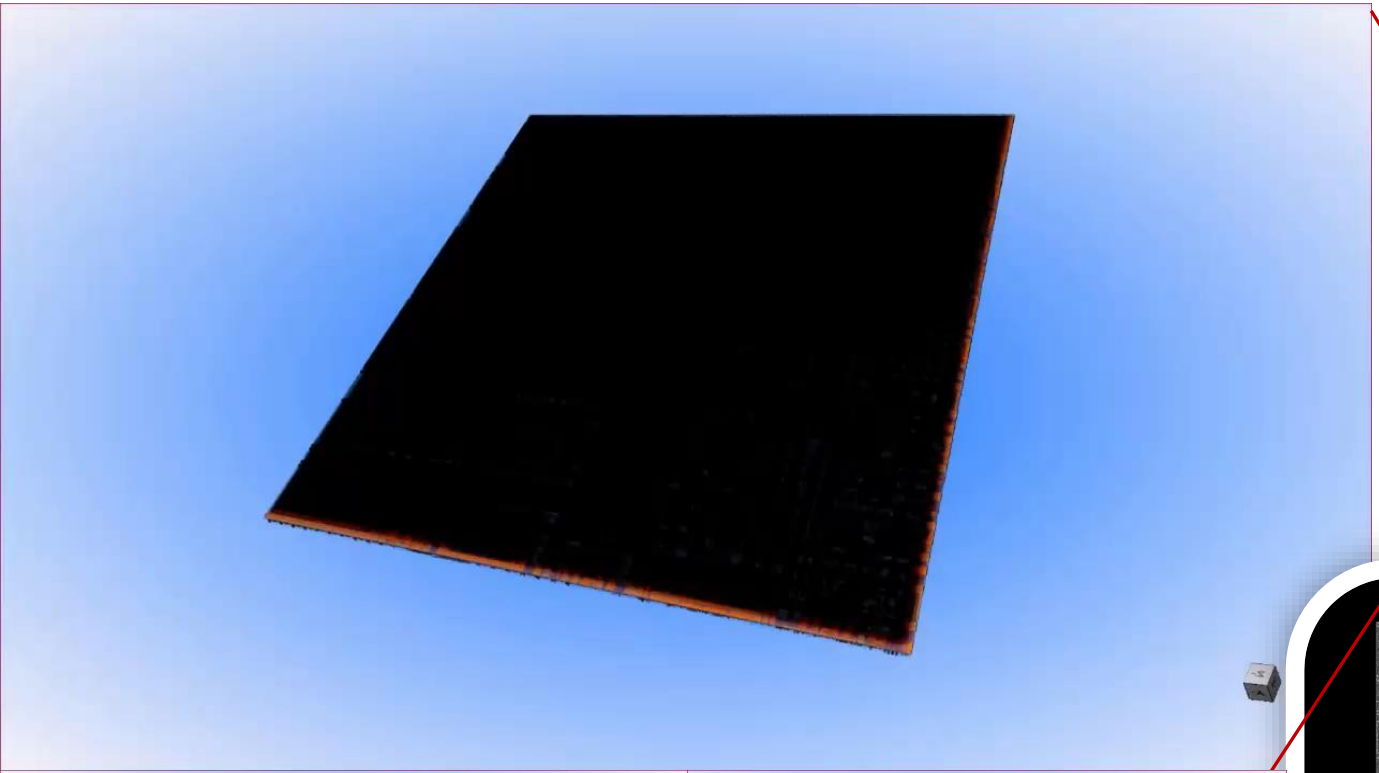
Protective mesh covering the top layer

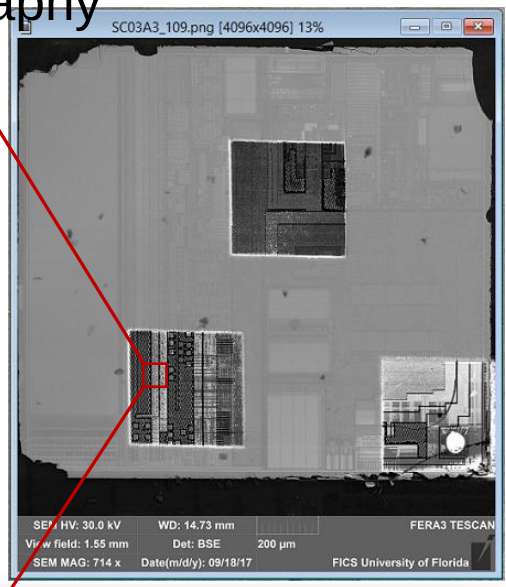


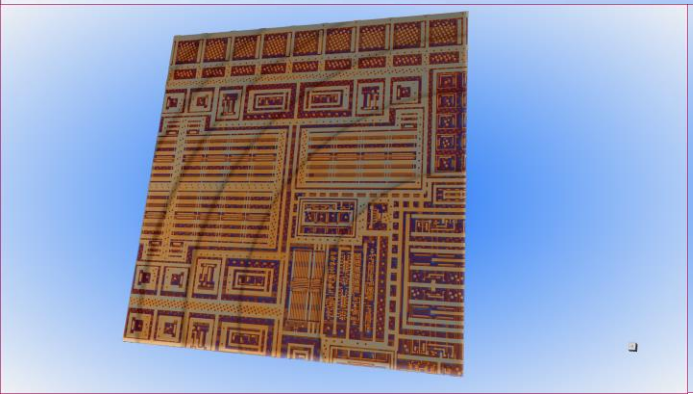


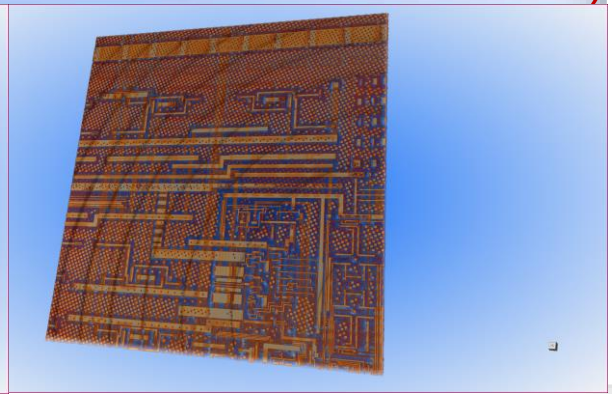
Case Study: Smartcard; Montage Tiles

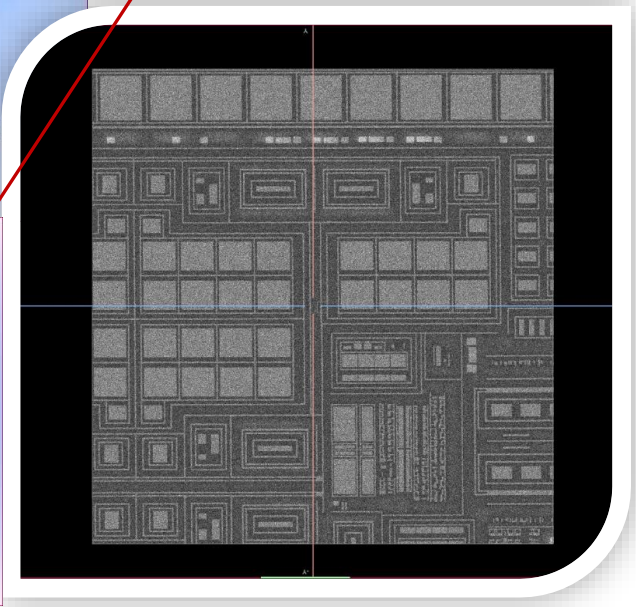
- 1st Examples of Automated Plasma FIB Delayer Tomography



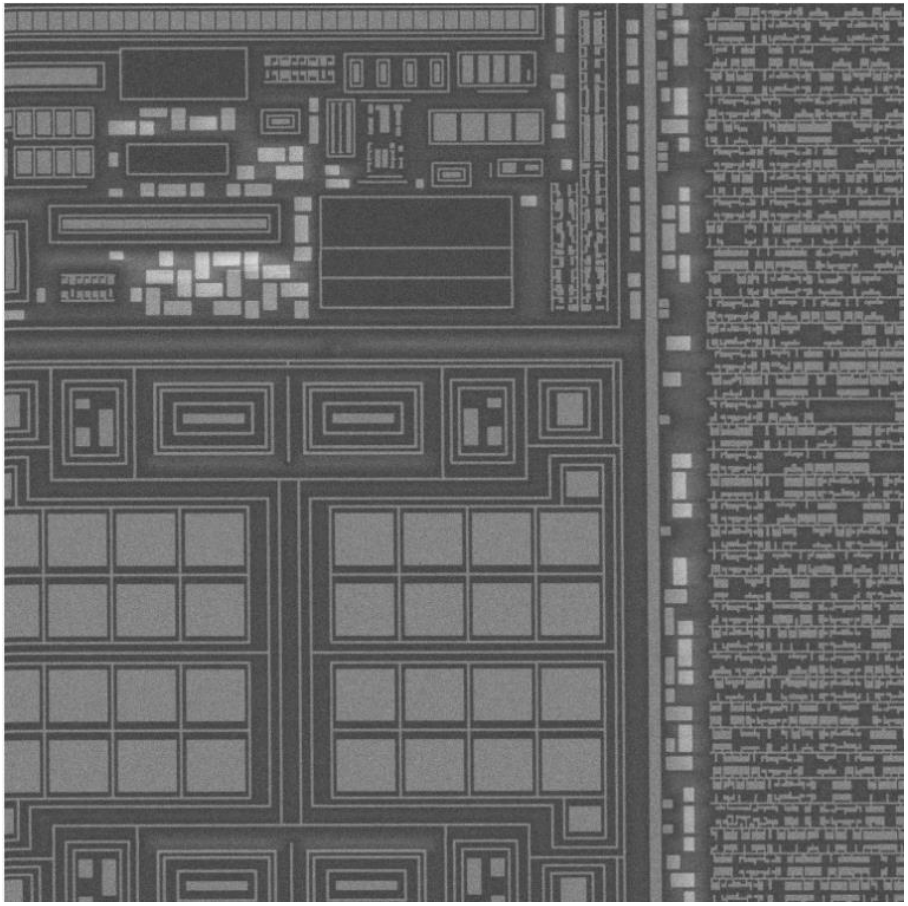




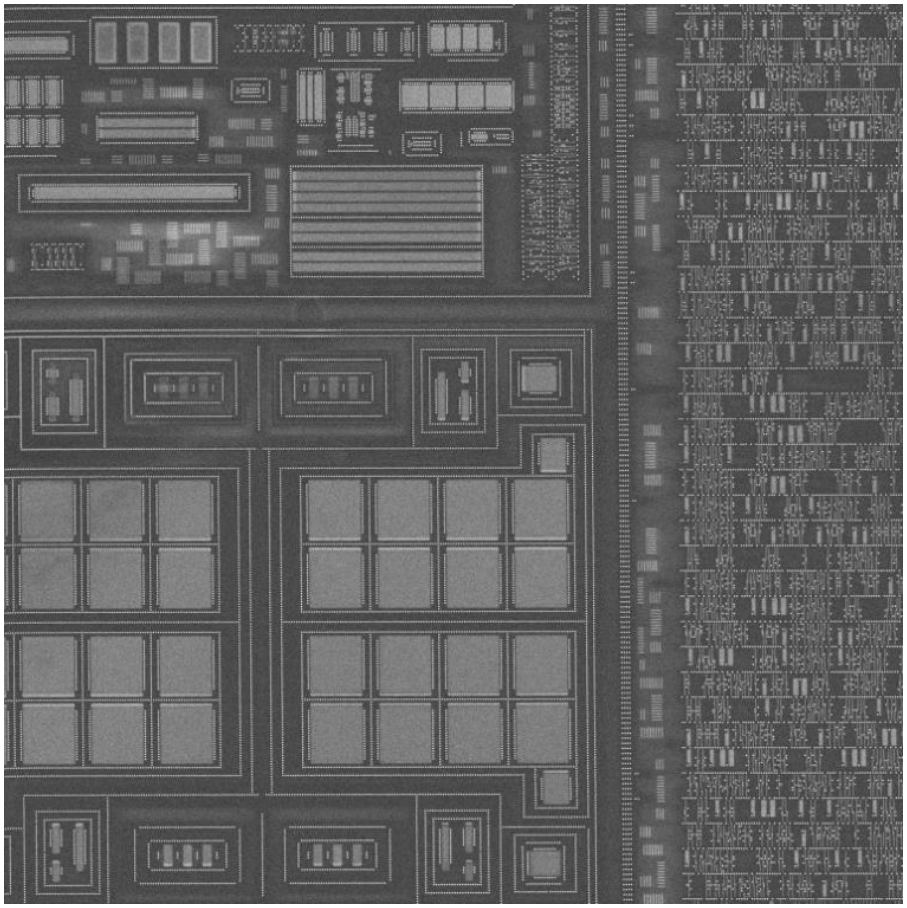




Case Study: Smartcard

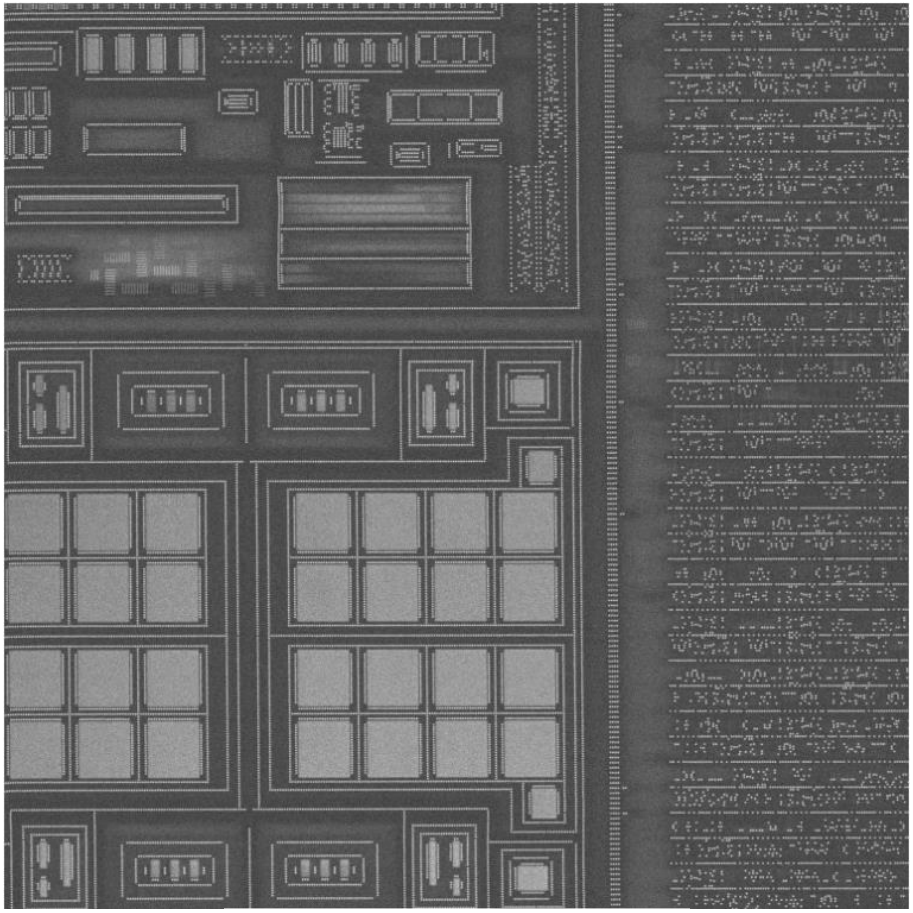


Doped

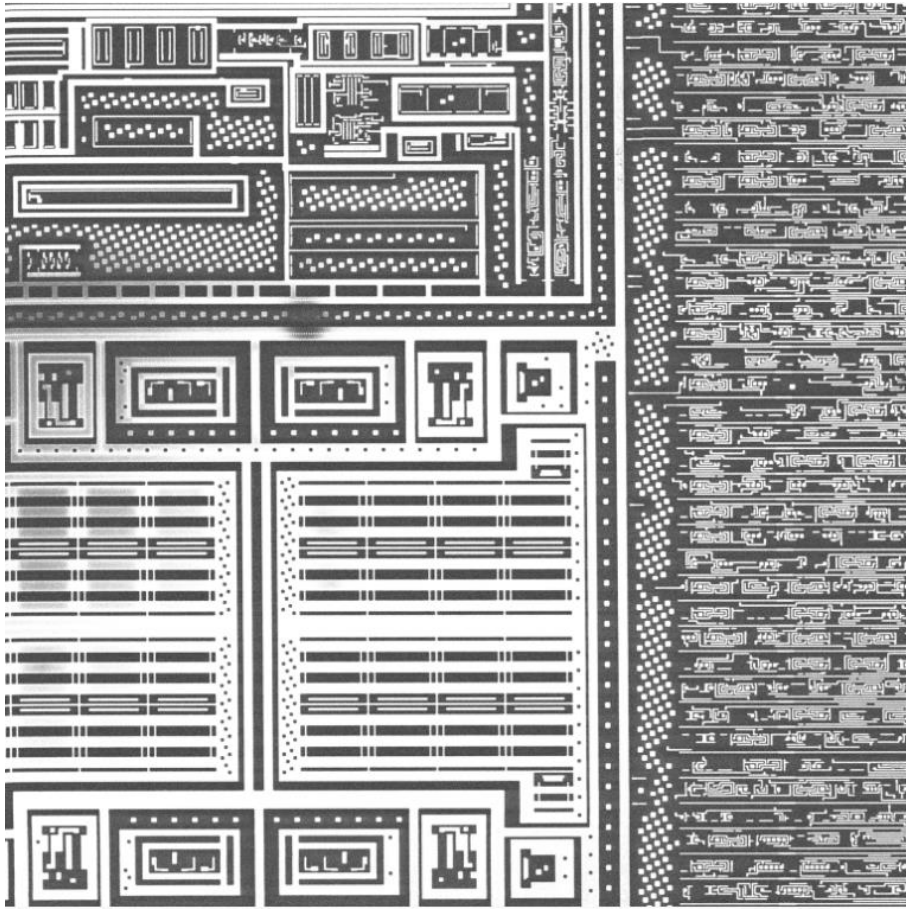


Poly

Case Study: Smartcard

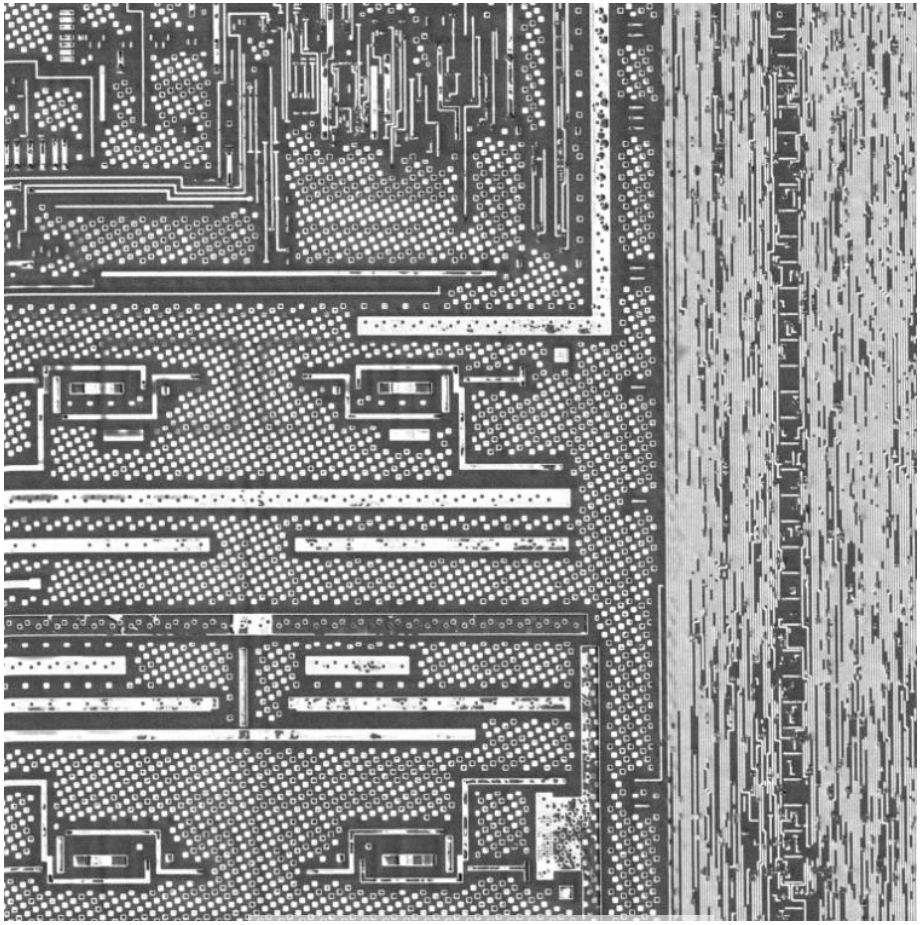


Contacts

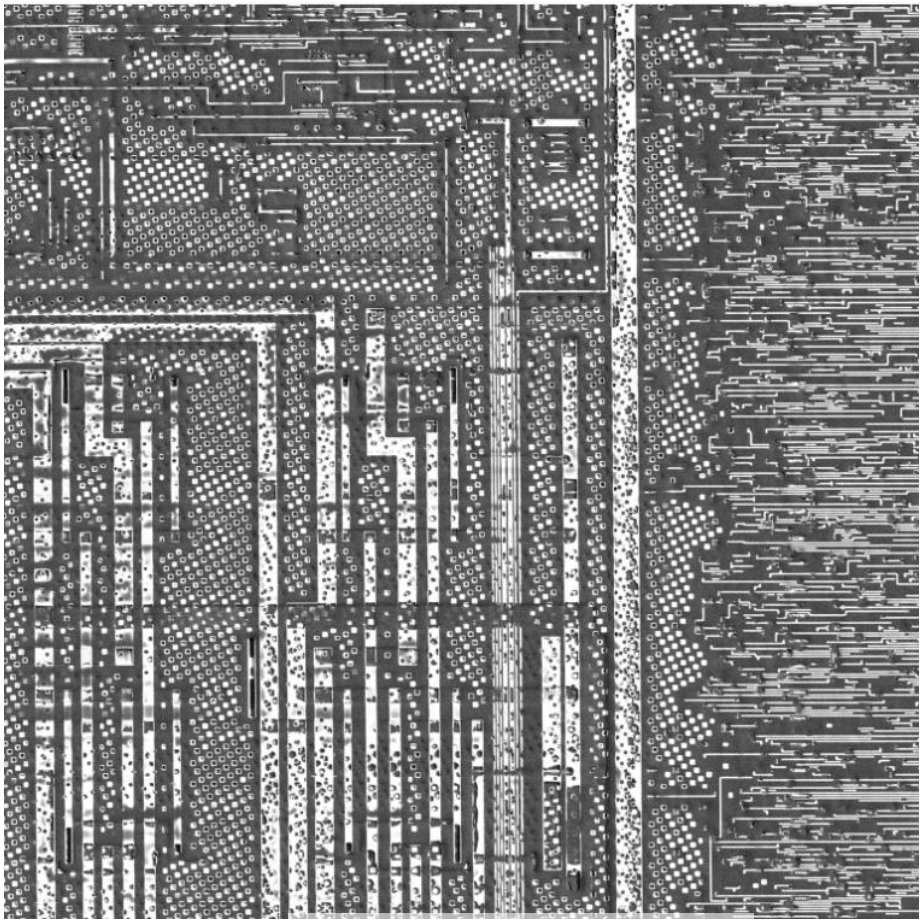


Metal 1

Case Study: Smartcard

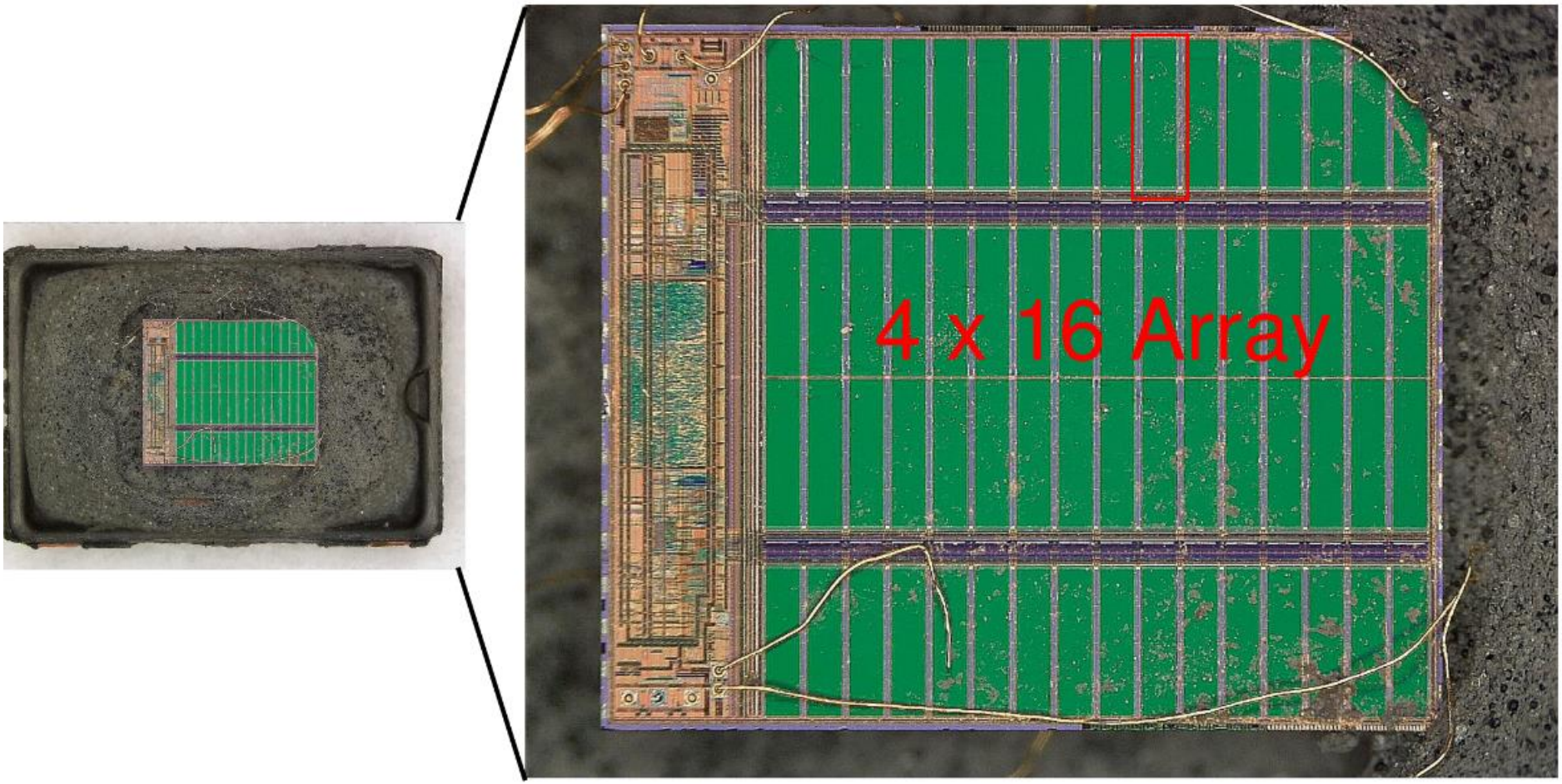


Metal 2

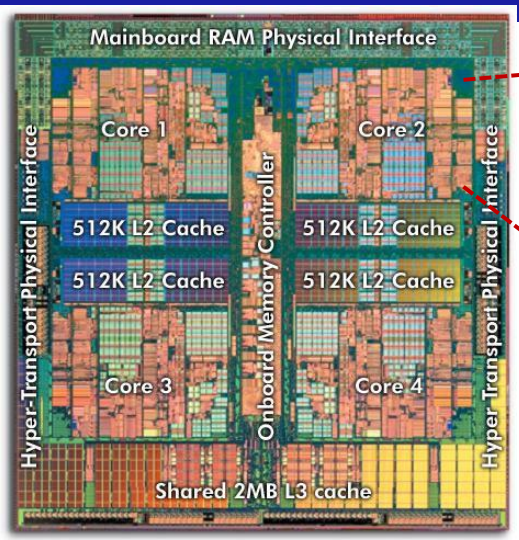


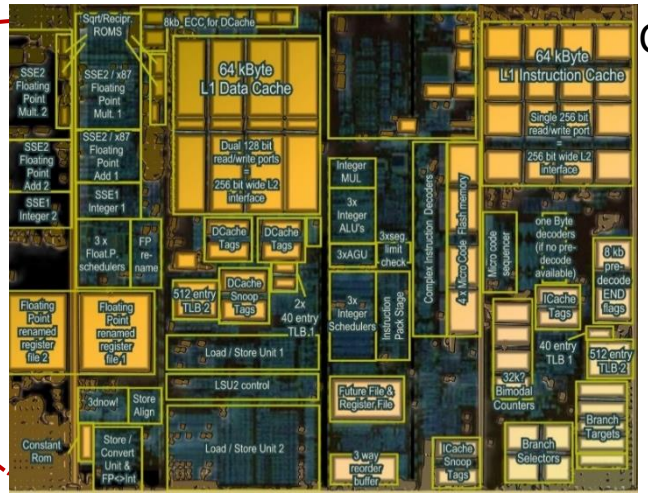
Metal 3

Flash Memory



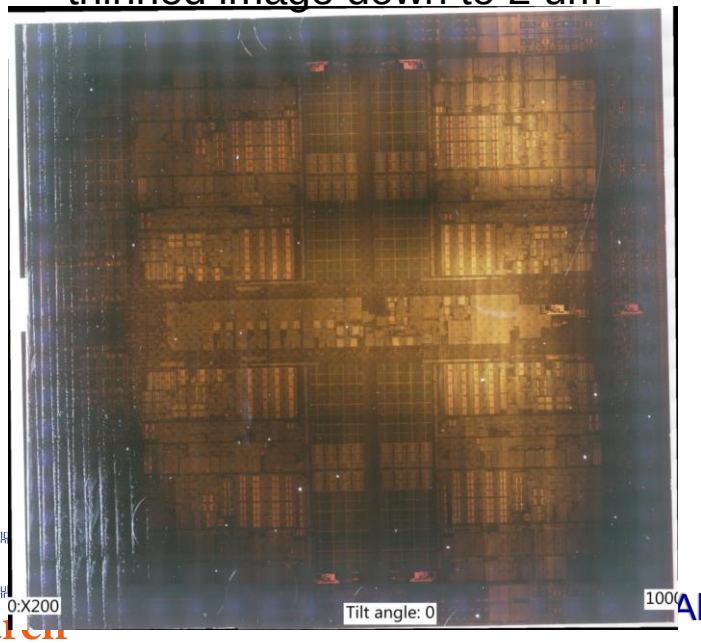
Opteron quad-core Barcelona



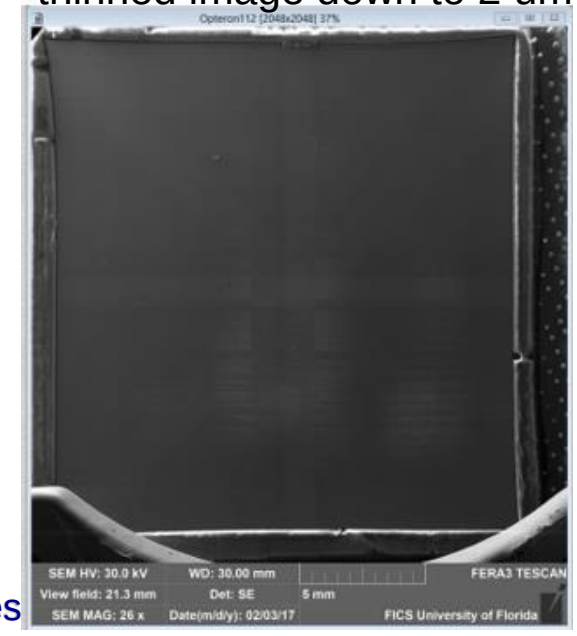


Core detail

IR image of the back side thinned image down to 2 um



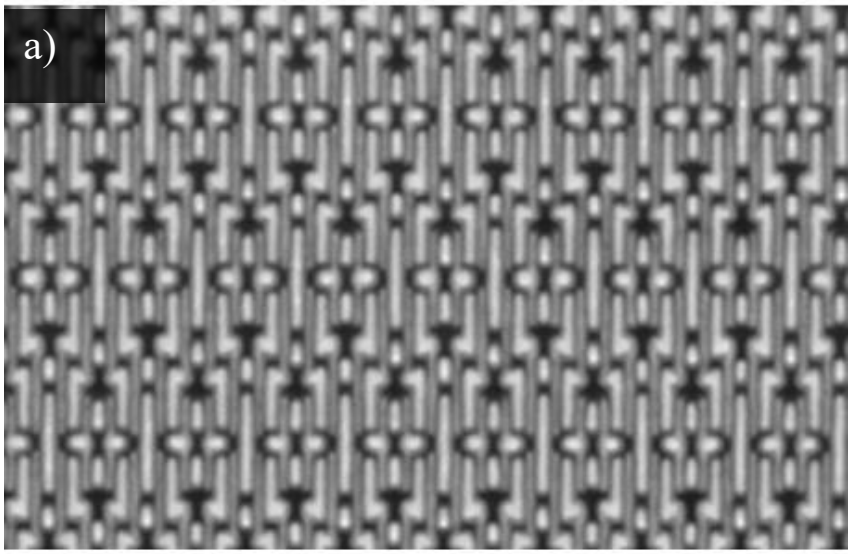
SEM image of the back side thinned image down to 2 um



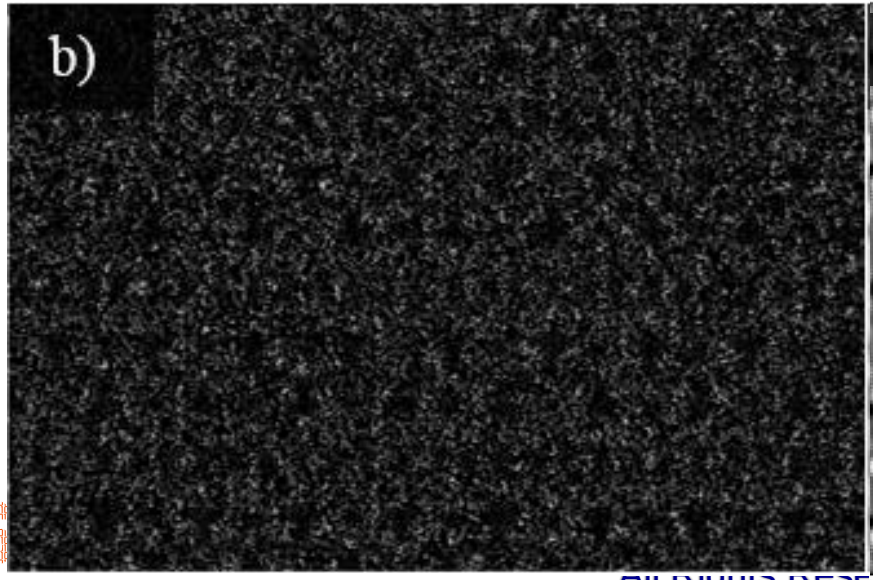
Compressed Sensing

- **Incorporation of "Intelligent Microscopy"**
  - Stage scanning, Adaptive milling strategies, Adaptive gas chemistry strategies, Adaptive data sampling strategies, data validation, etc.

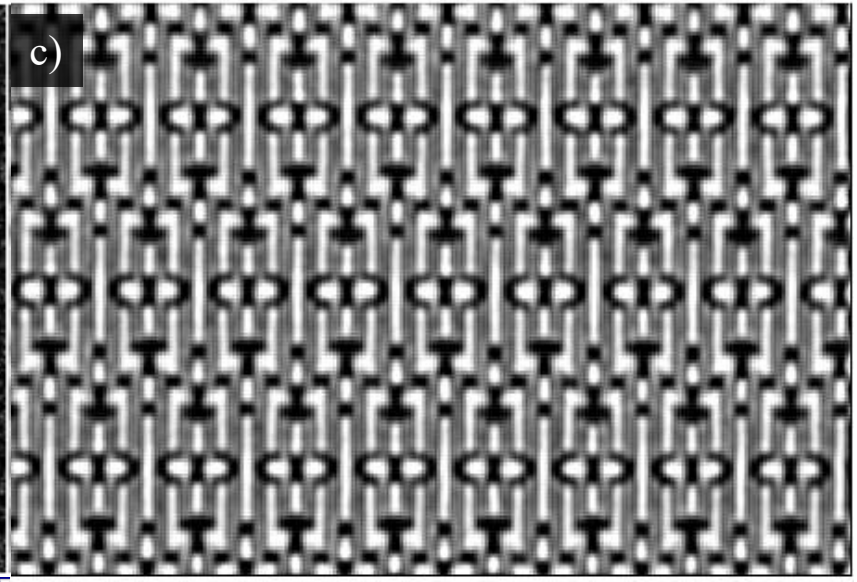
original image



20% of original data acquired

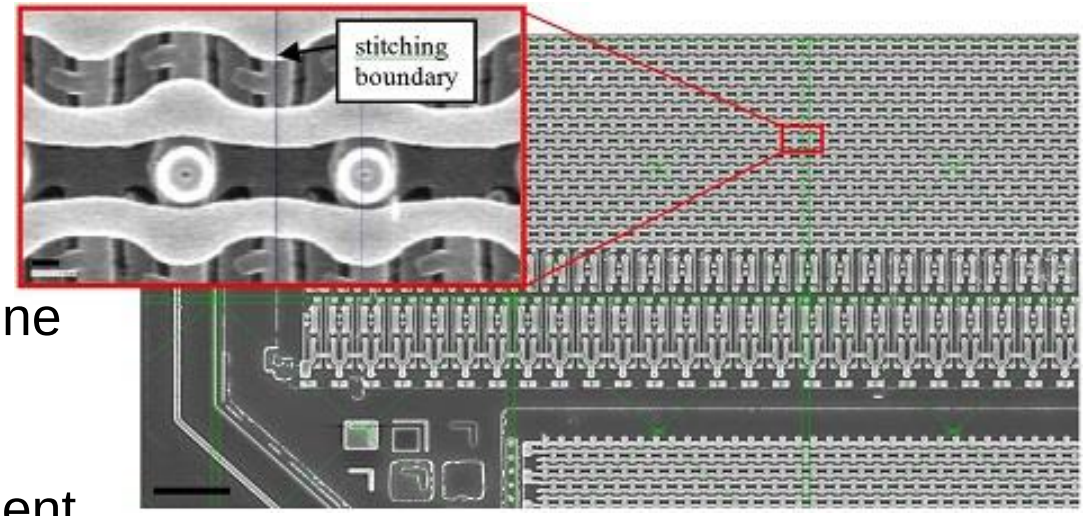


recovered - with decon.



Layer reconstruction. Mosaicking

Most approaches to image stitching require nearly exact overlaps between images



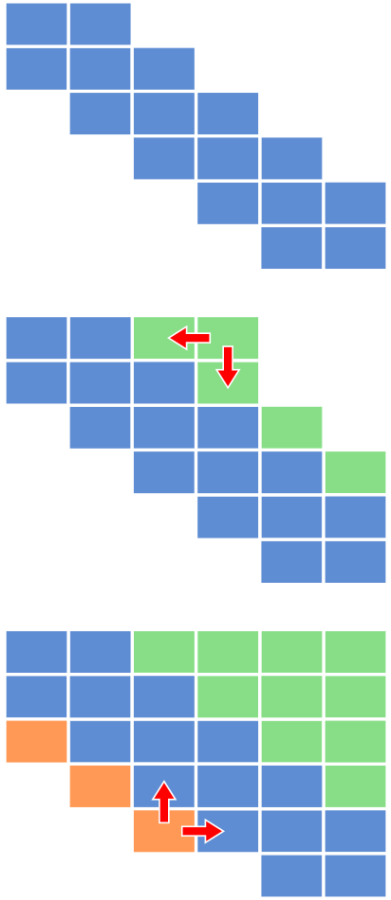
Stitching steps:

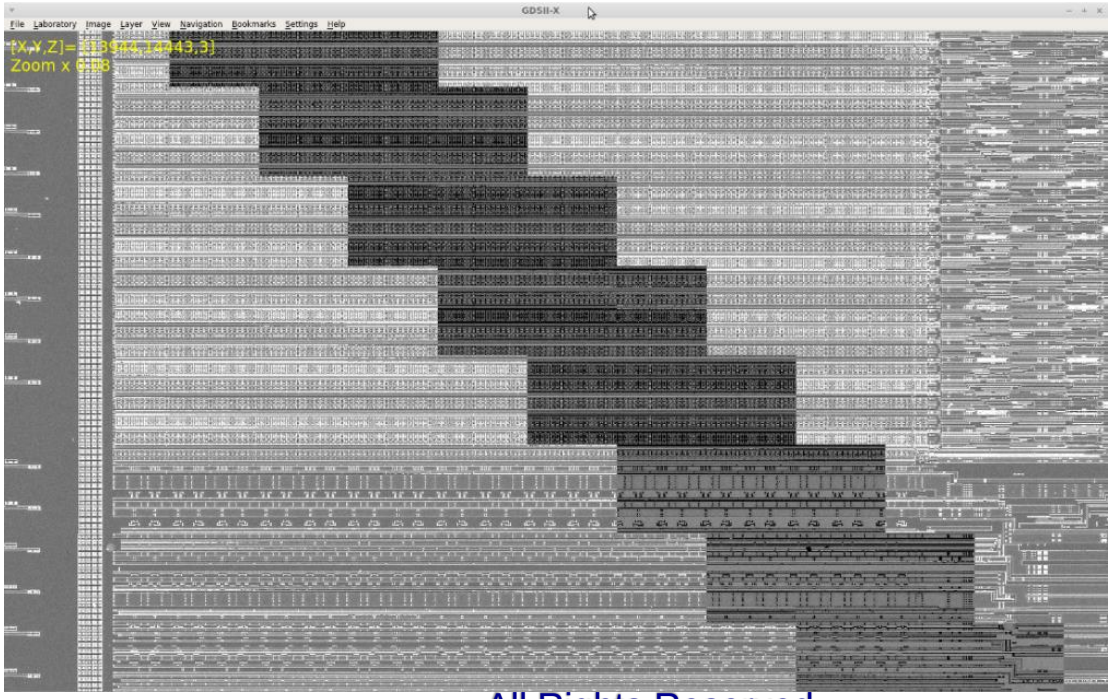
1. Image alignment to determine the pixel coordinate on two images
2. Estimate the correct alignment to combine pixel to pixel comparisons (using optimization technique like gradient of the image)
3. Extract distinctive features to efficiently match pairs
4. Count in the image distortion, exposure difference, image drift, etc.

- Stitching using laser interferometer stage coordinate as a side information
- Repetitive features creates problem with stitching

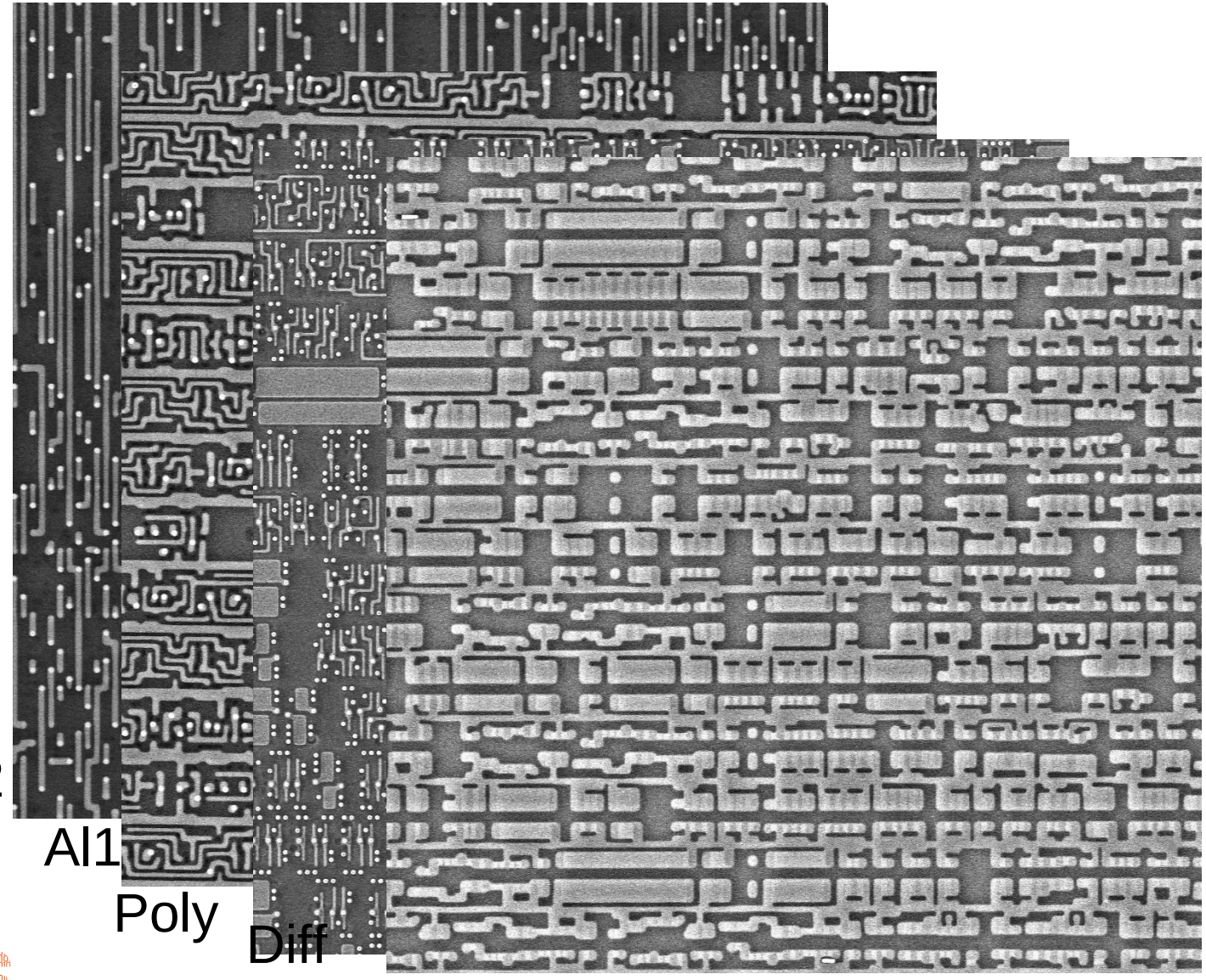
Layer reconstruction. Mosaicking

- Mosaicking starts with the ‘backbone’ creation
- Tiles are sequentially added
- Stitching decision changed on adjacent tiles, avoiding error propagation





Physical Layer Overview

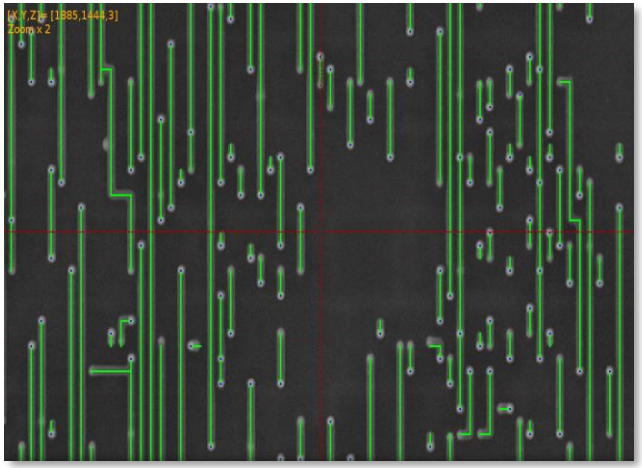


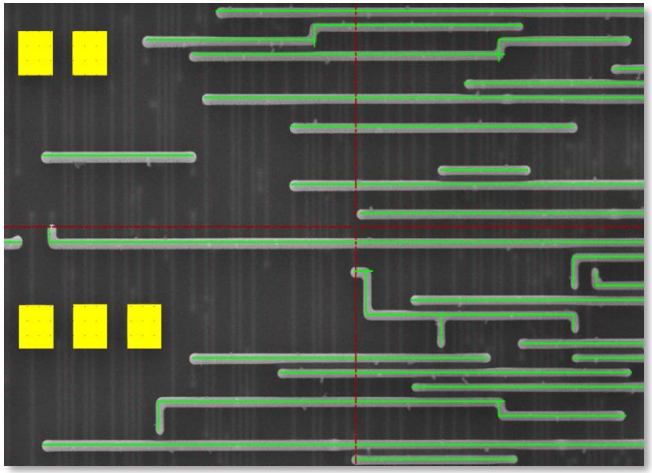
Polygon Extraction

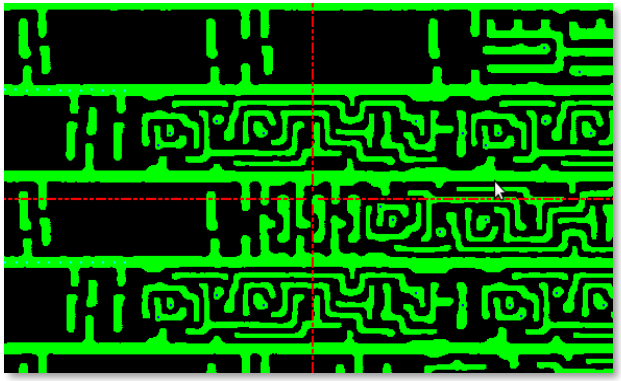
- Tile-image **segmentation** process

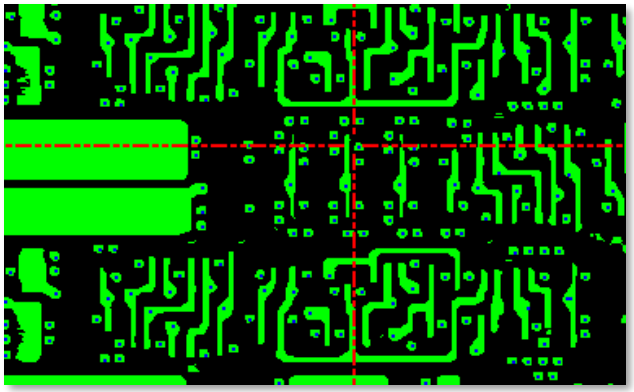
- Detection of:

- Regular horizontal **routing**
- Vertical **vias**
- **Supply** rails
- **Dummy** filling
- **Poly**
- **Doped region**

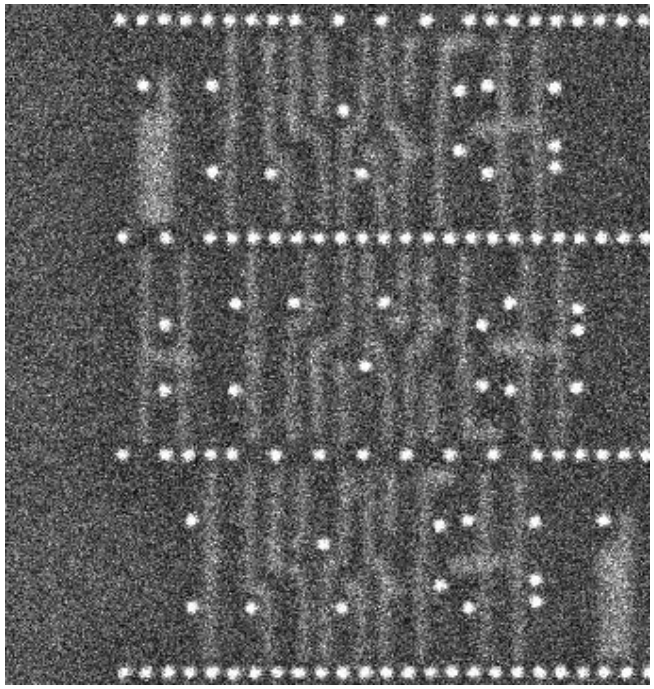




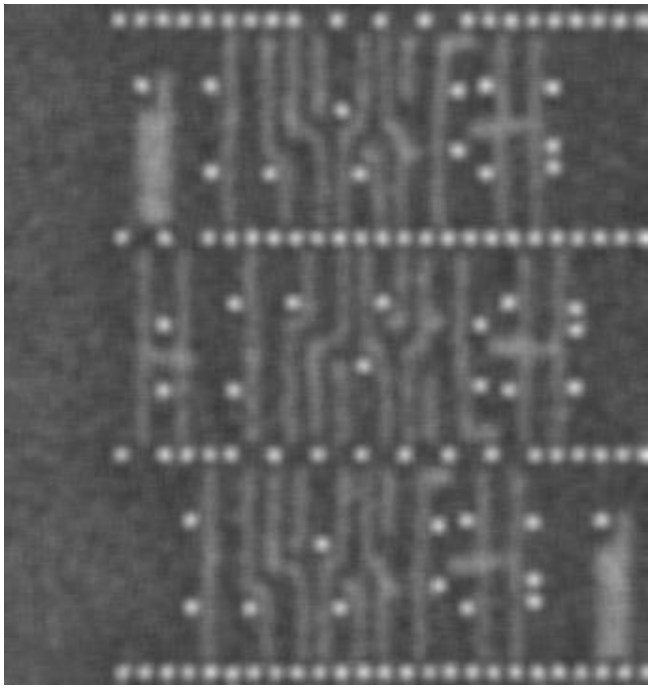




Box Filter



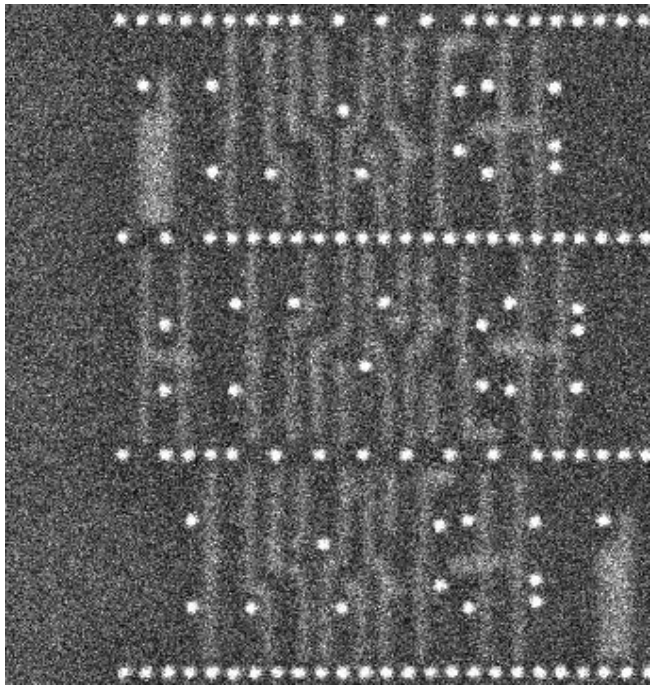
Original image



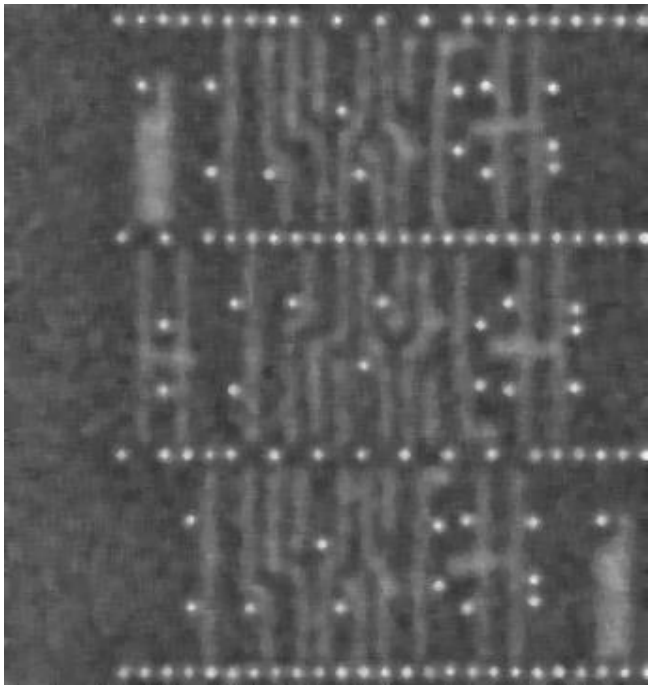
Filtered image

Box filter aka Mean Filter replaces the value of each pixel with the mean of the values inside the kernel.

Median Filter



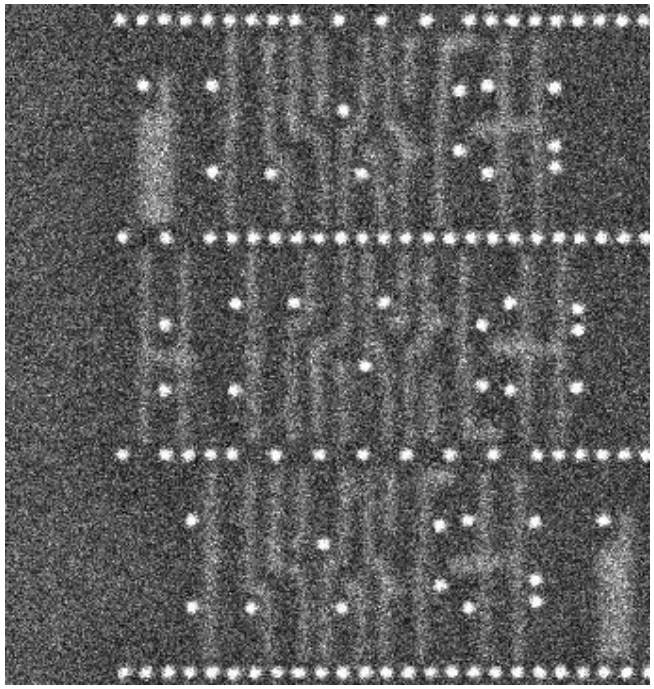
Original image



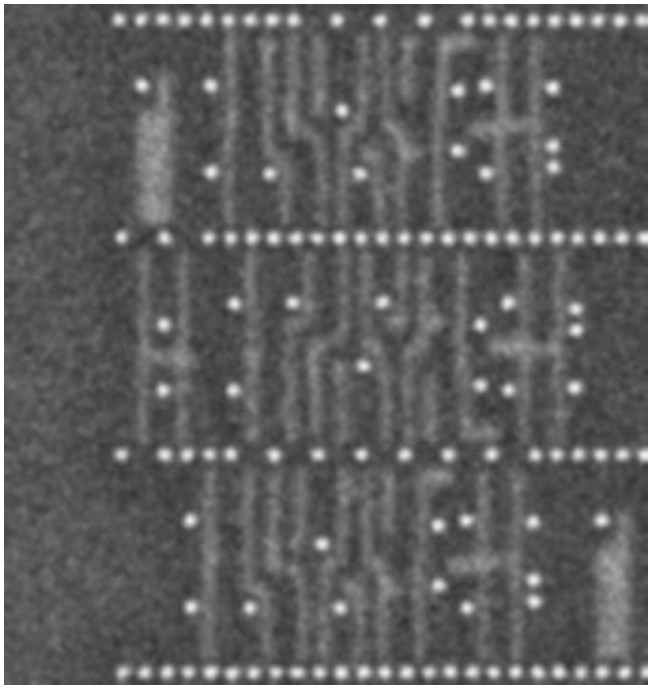
Filtered image

Each pixel in the image is replaced by the median of the pixels in the kernel. Mostly effective against salt and pepper noise.

Gaussian Blur



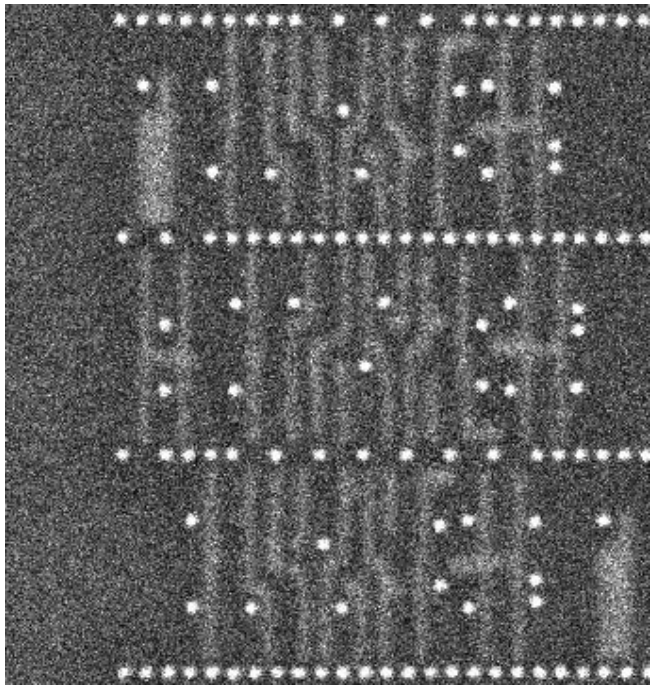
Original image



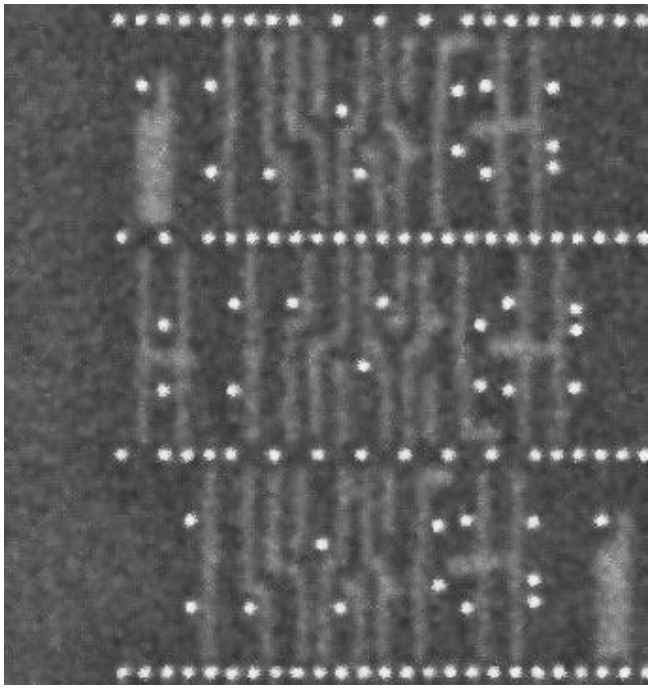
Filtered image

Image convolved with Gaussian Kernel with same/different standard deviation on the axes. Effective against Gaussian noise.

Bilateral Filter



Original image



Filtered image

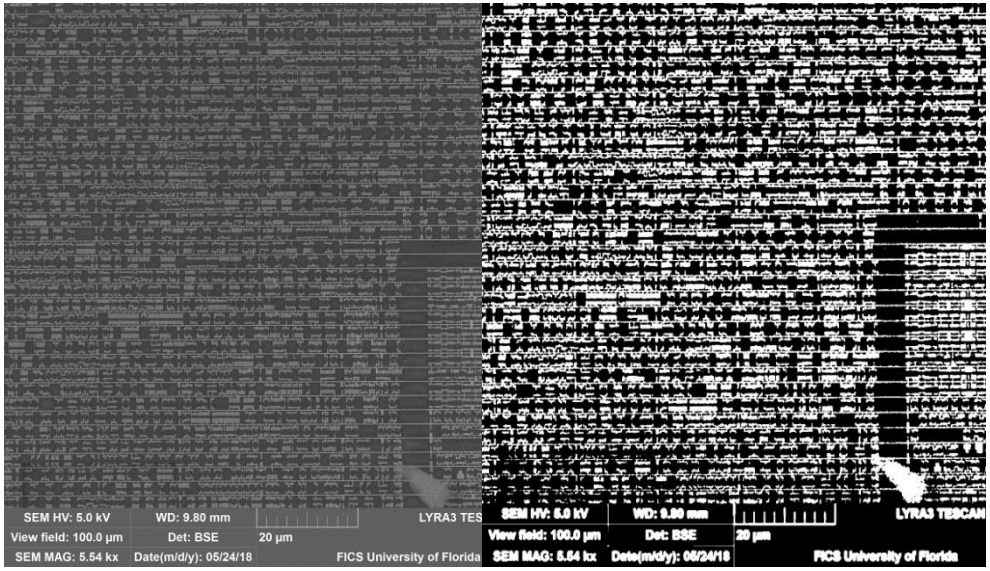
Special type of filter that detects edges and blurs the image conserving the edges. Effective for removing textures from images.

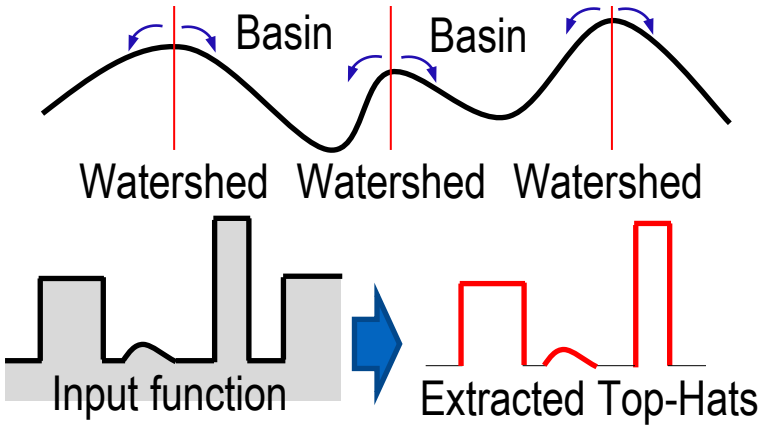
Segmentation Techniques

De-noising
- Anisotropic
- Edge preserving
- Deblur
- Etc.

Edge detection
- Sobel
- Hugh transforms
- Image gradient
- Etc.

Segmentation
- TopHat
- Watershed
- Binarization
- Etc.

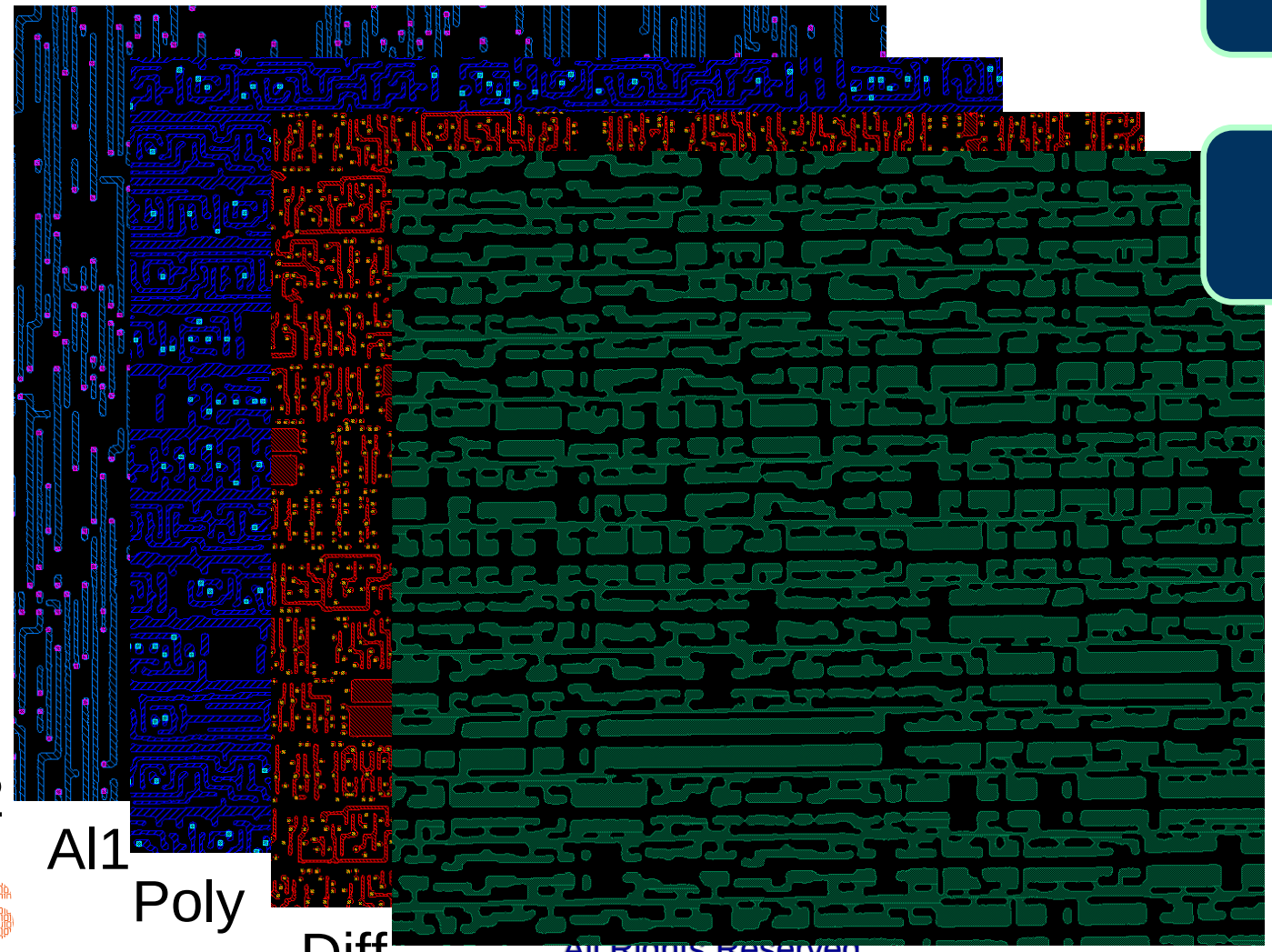




Polygon Extraction

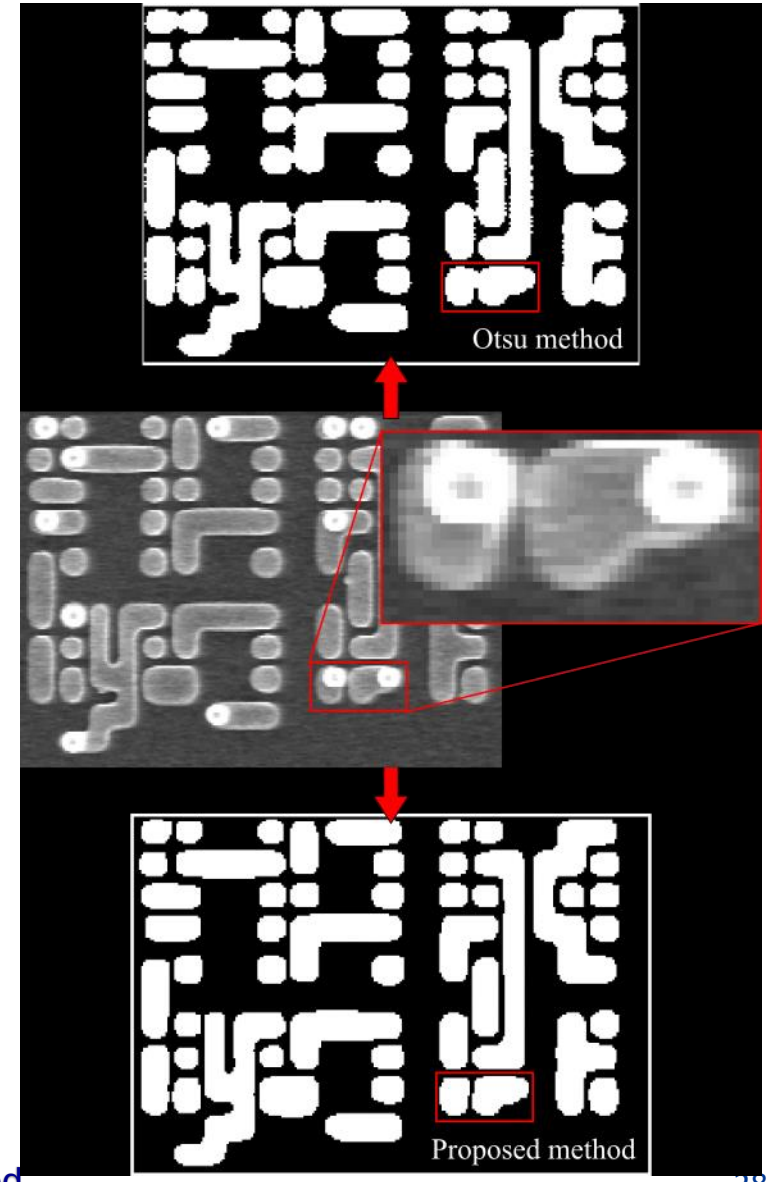
SEM Physical Imaging

Mask layout



Geometry Extraction. Machine Learning

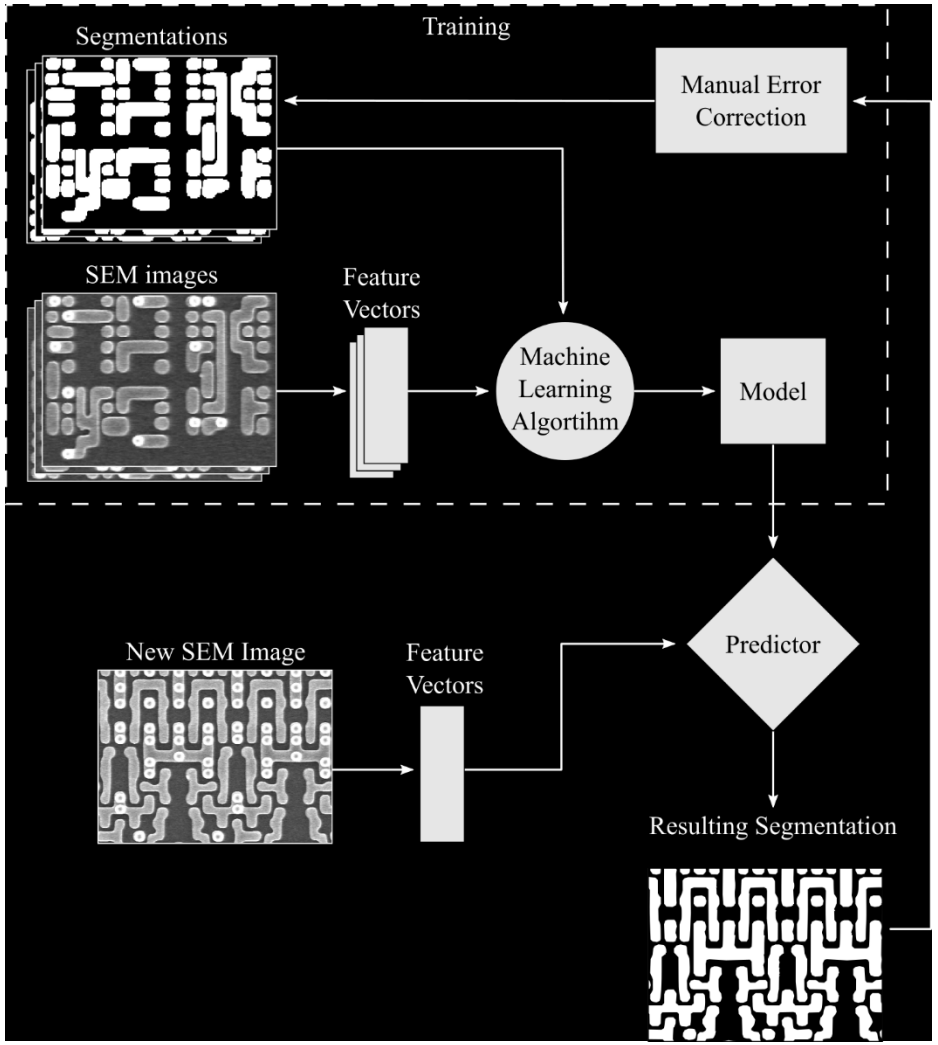
- There will be errors during regular image segmentation
- Machine learning is a proper solution to solve such errors
- User must train the model for each new technology
- Critical geometries will be rightly segmented
- Deep learning methods can be used to detect ‘complex’ structures, such as dust or RIE artifacts



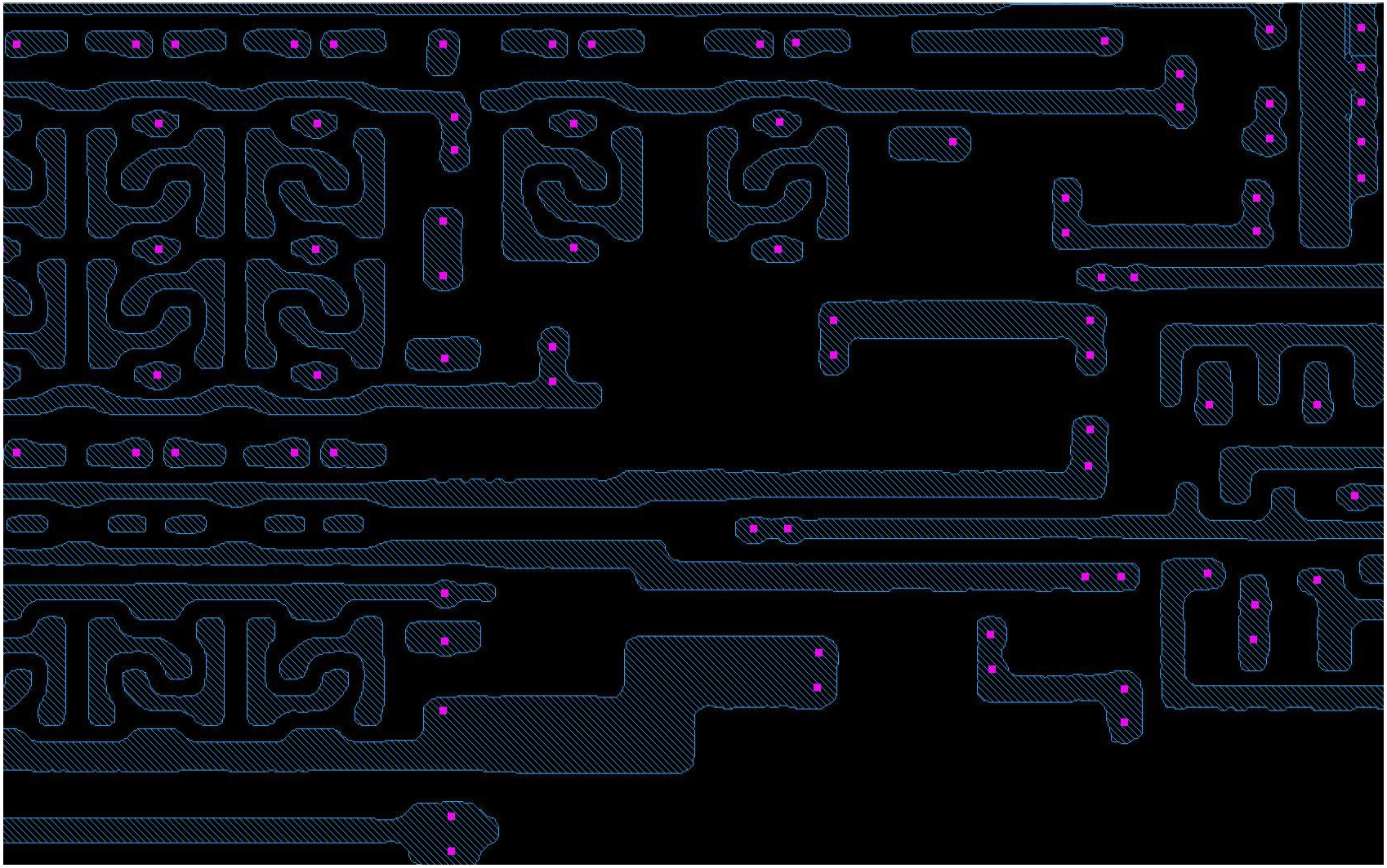
Geometry Extraction. Machine Learning

- **Automated layer vectorization (GDS) is mandatory for large IC area reverse engineering**

- Classic intensity-based segmentation methods need heavy tuning for each new technology or layer
- AI-based segmentation methods highly reduce the human interaction
- User must define the full/empty shapes in a few examples and supervise the prediction results



Geometry Extraction. Machine Learning

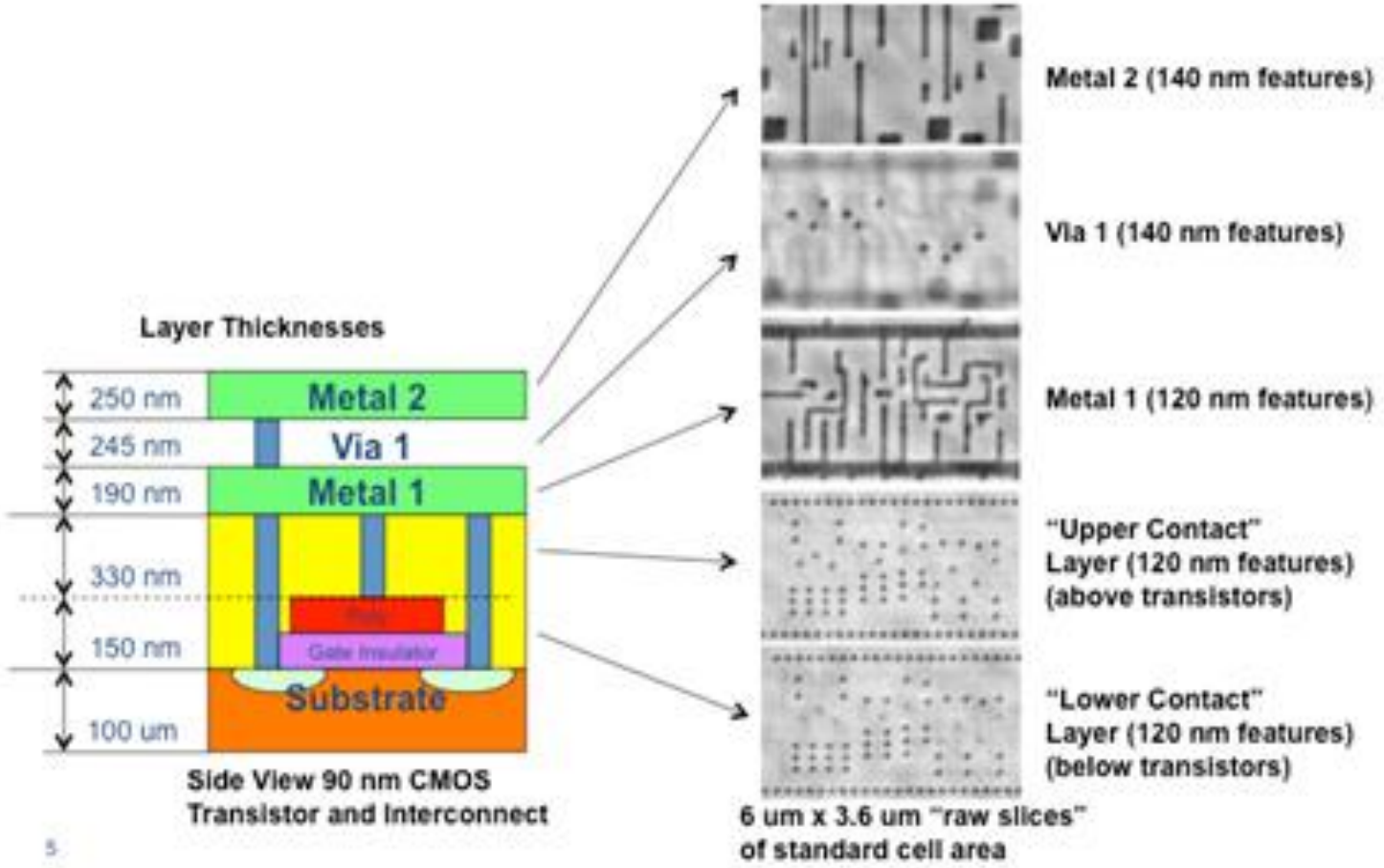


Geometry Post Processing

- Smart polygon simplification
- Always there will be errors!
  - Segmentation errors
  - Bad layer stacking
  - SEM artifacts
  - Dust
- Via layers used to recompute global layer distortions
- Multi layer boolean and DRC-based operations to find errors
- … but still manual error correction needed
- And still there will be errors!
  - ERC-based check after gate extraction
  - Worst ones are discovered in functionality extraction phase

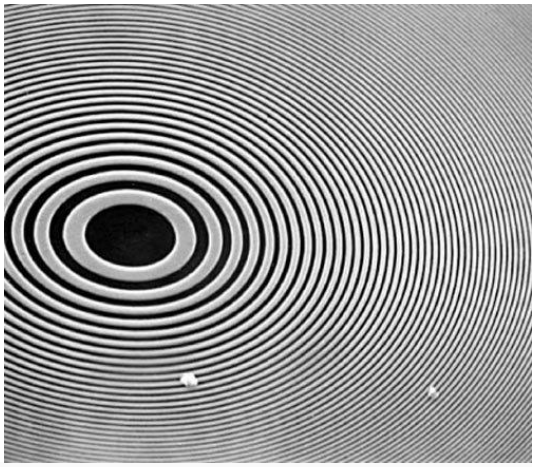
X-rays for IC Reverse Engineering

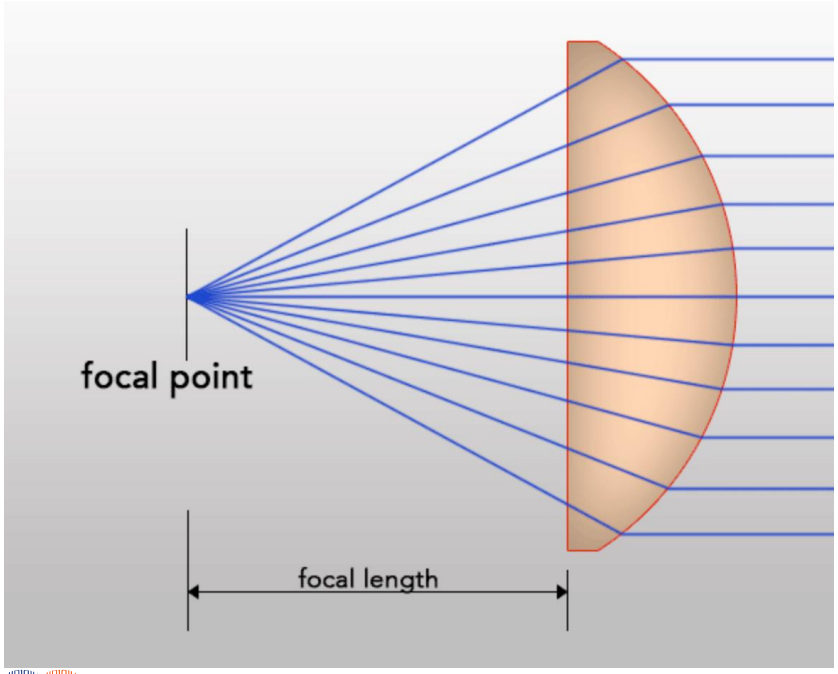
Nano X-ray Tomography

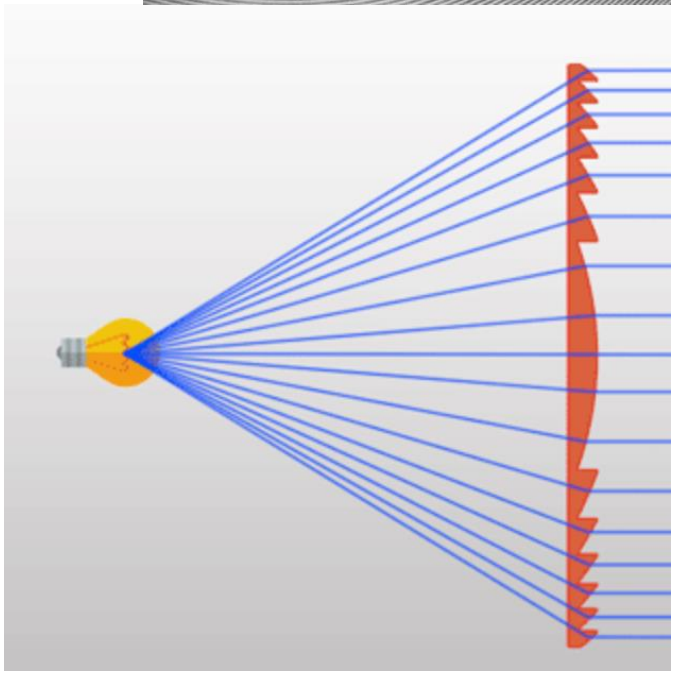


Nano Focused X-rays

- Modern X-ray optics paired with synchrotron light sources can create very small spot size
- With Fresnel zone plates and Kirkpatrick–Baez mirror pairs 7 nm spot size is created at 20 keV;



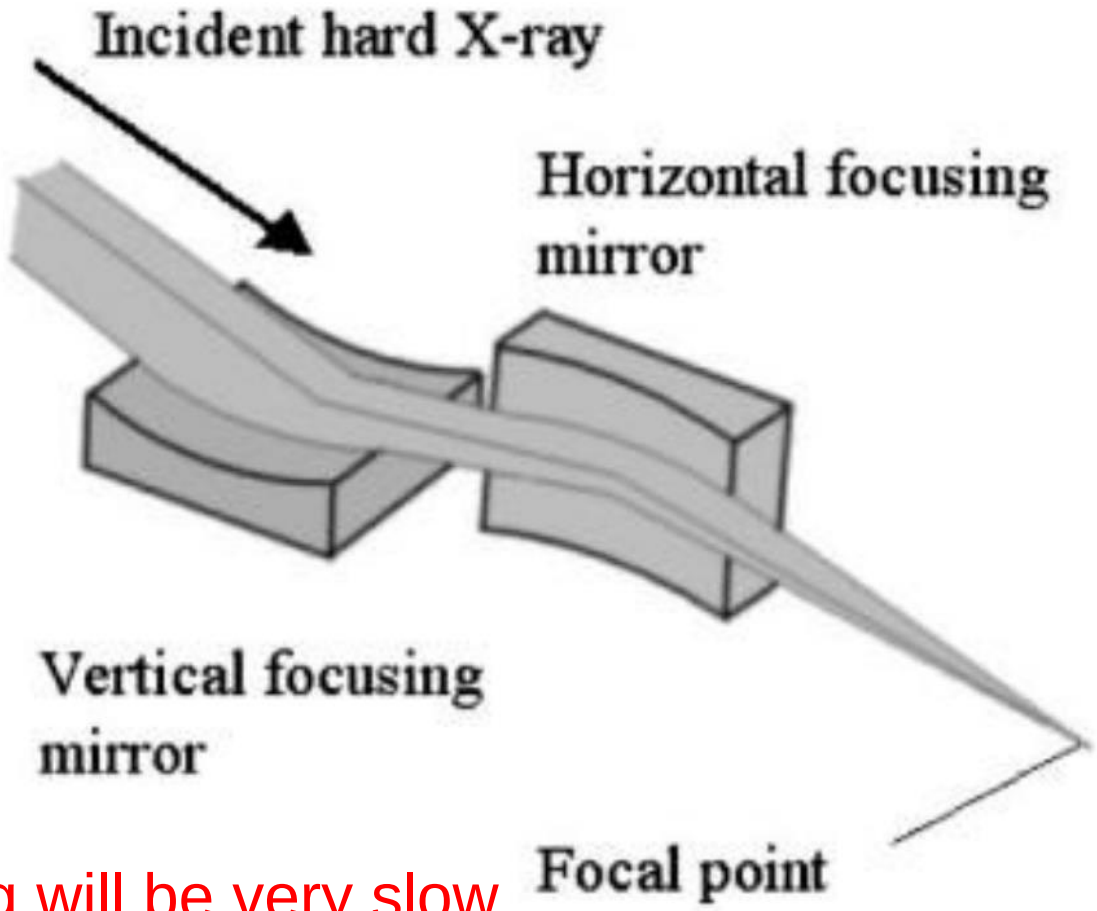




Nano Focused X-rays

K-B mirrors

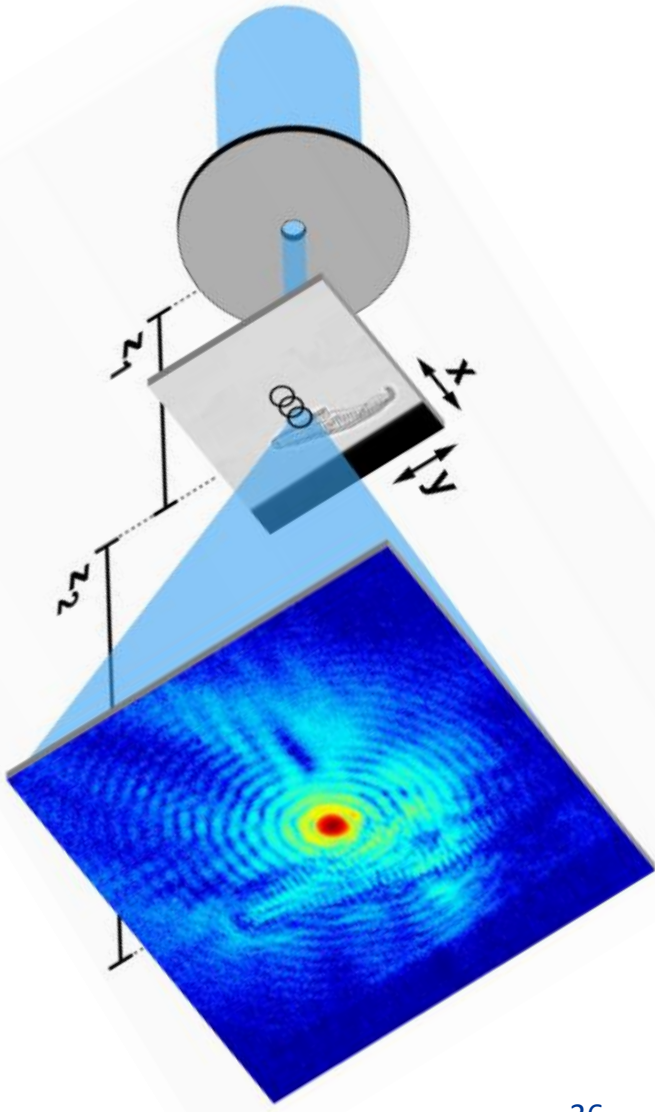
- consists of two curved mirrors placed at right angles to each other.
- coated with a layer of a heavy metal
- Can focus beams to small spot sizes with minimal loss of intensity



Nano X-ray imaging will be very slow to do tomography on ICs

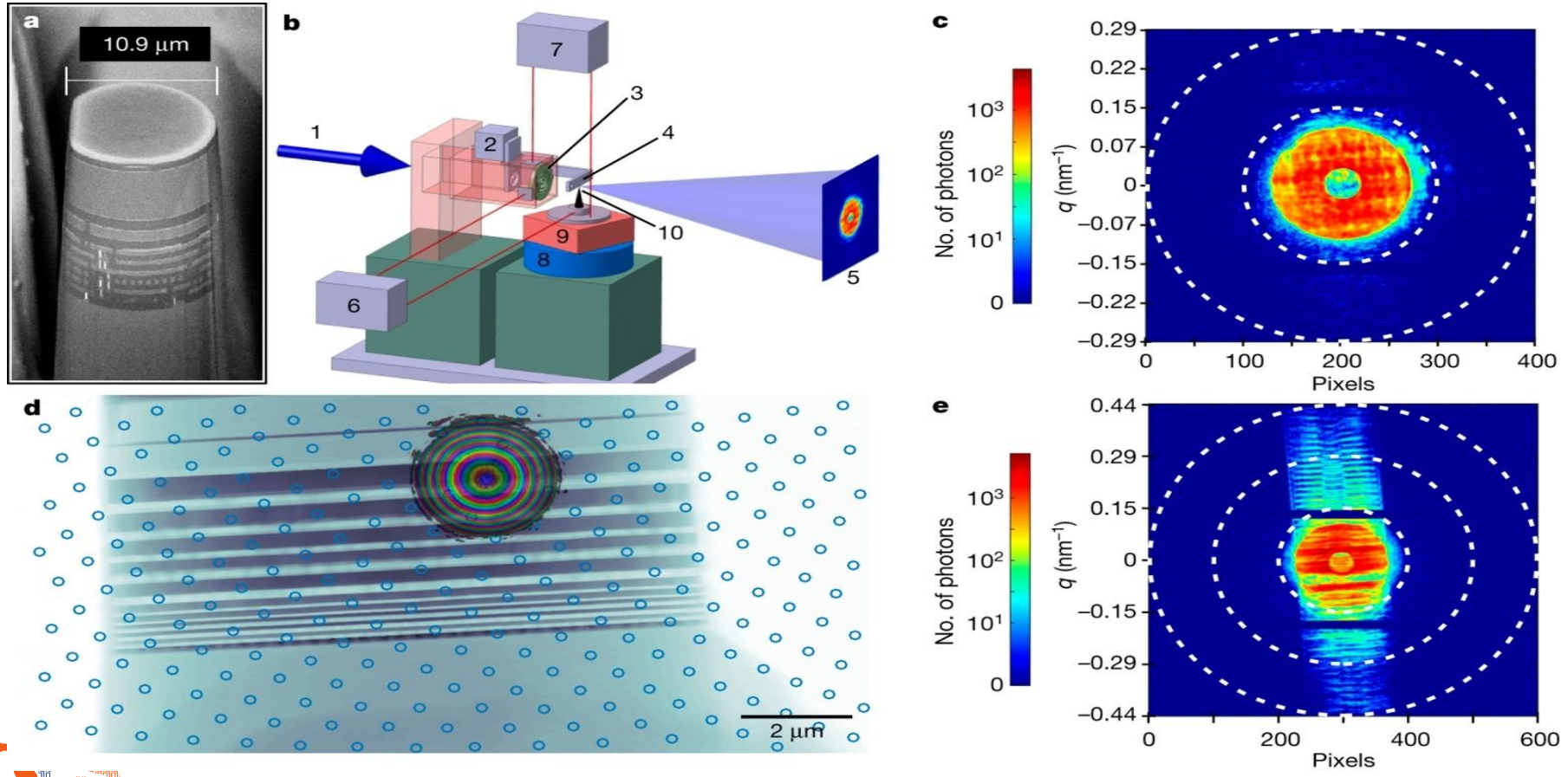
Ptychography

- Illuminate an object with a beam
- Collect huge diffraction pattern downstream
- Diffraction pattern contains all information about the region of object illuminated
- The image includes the amount of energy and spatial frequency inside the ROI
- The middle of image contains low frequency features
- And far away contains high frequency details of object



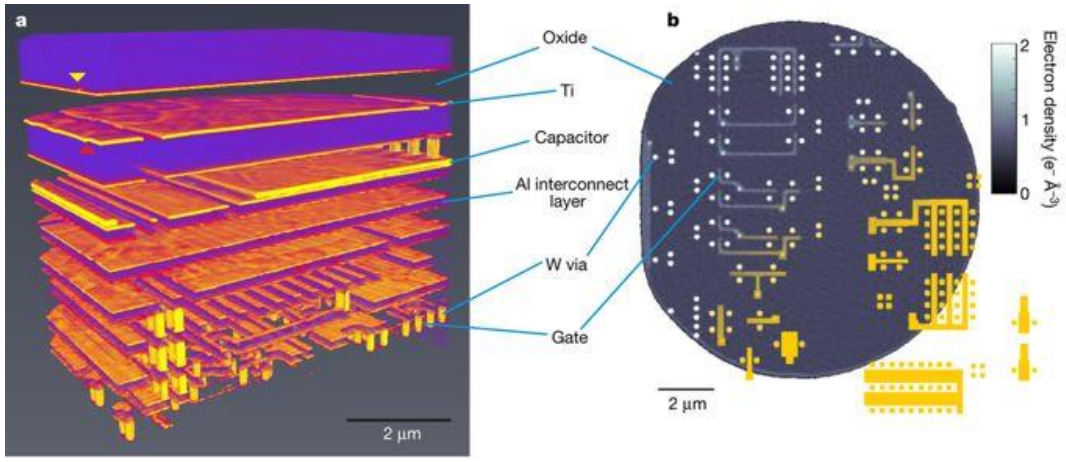
Ptychographic X-ray Computed Tomography

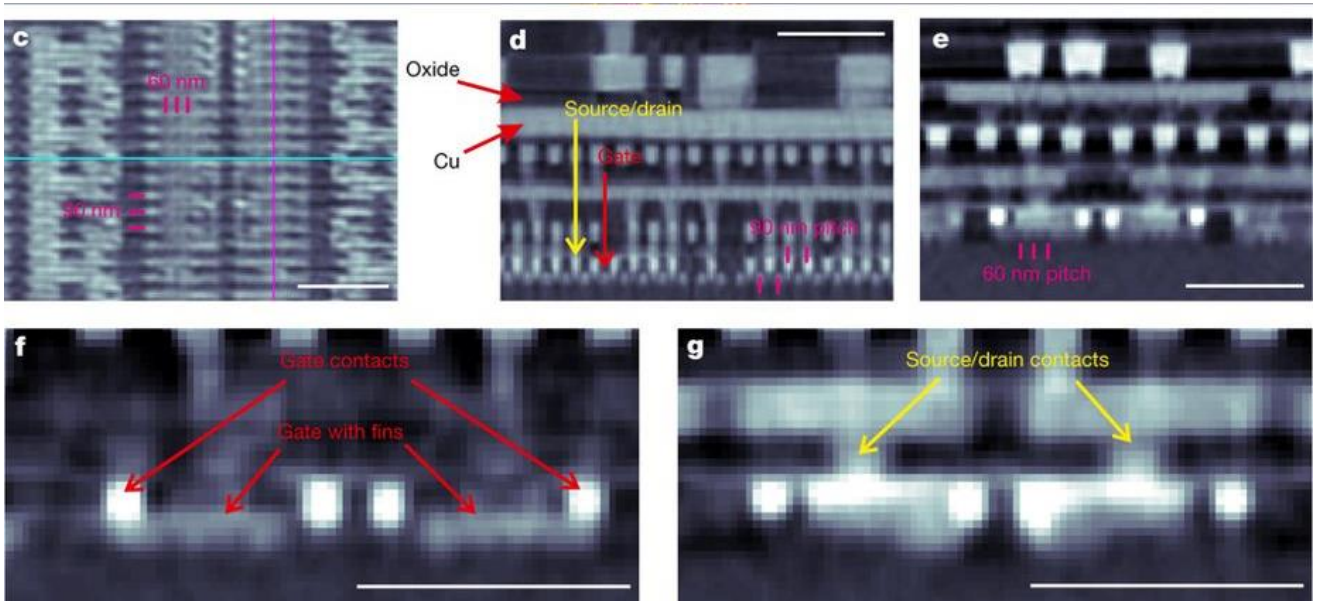
- Sample is scanned with a coherent X-ray beam
- At each location a 2D diffraction pattern is recorded in far field regime
- Using numerical reconstruction algorithms, the object's complex transmissions function and the illuminating wave field can be reconstructed from series of diffraction patterns.



Ptychographic X-ray Computed Tomography

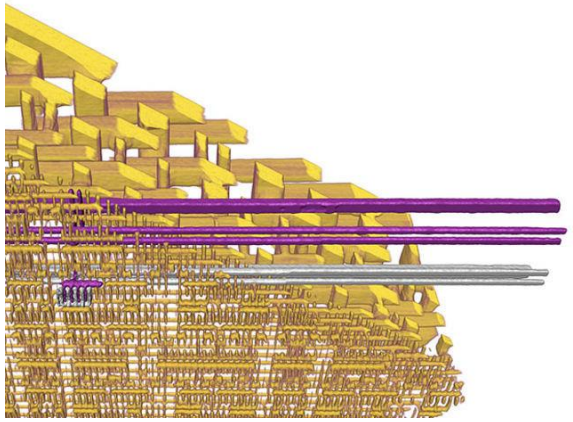
- Ptychography can resolve structures in the sample that are much smaller than the beam size.
- However the biggest challenge is the sample size

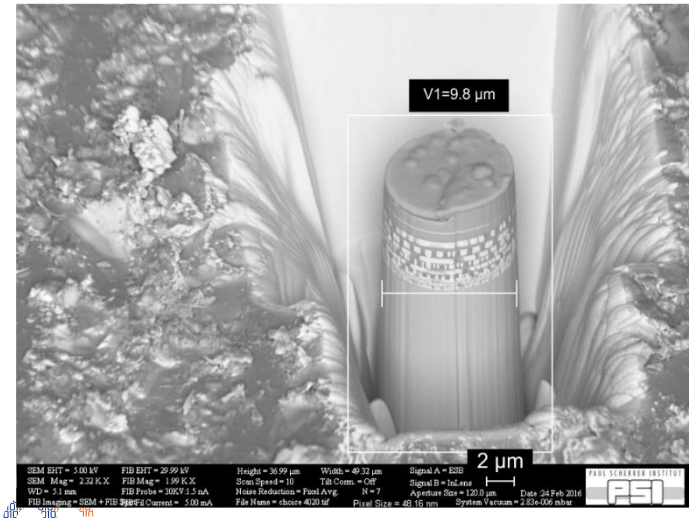


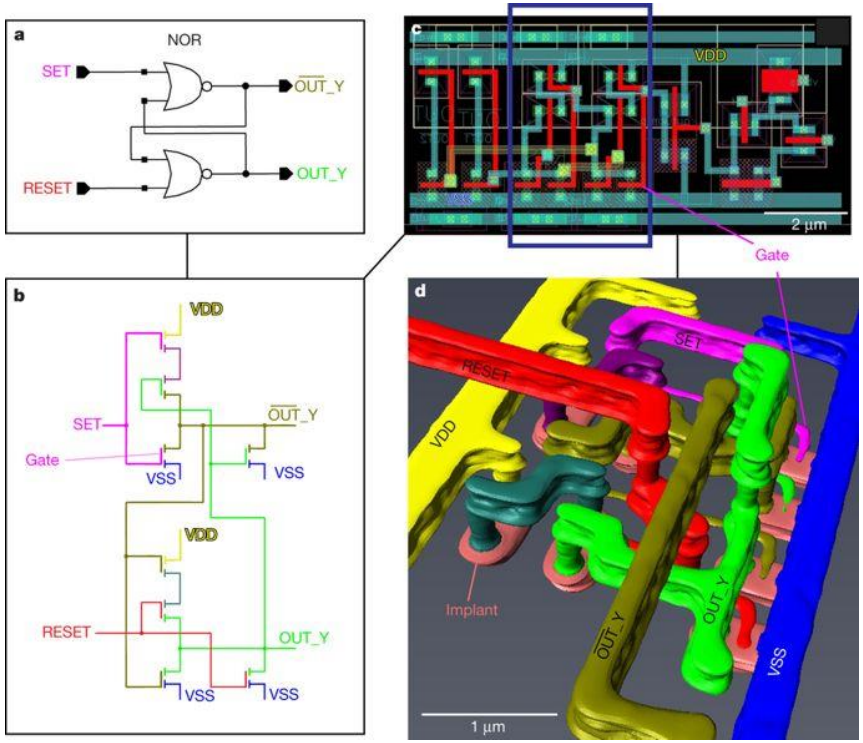


Ptychographic X-ray Computed Tomography

- Ptychography can identify material by having prior information of candidate materials.
- Samples need to be as small as few tens of microns







- https://www.youtube.com/watch?v=VyQAg4j-7K4
- https://www.nature.com/articles/nature21698