IC Reverse Engineering Netlist Extraction Pix2Net Demo

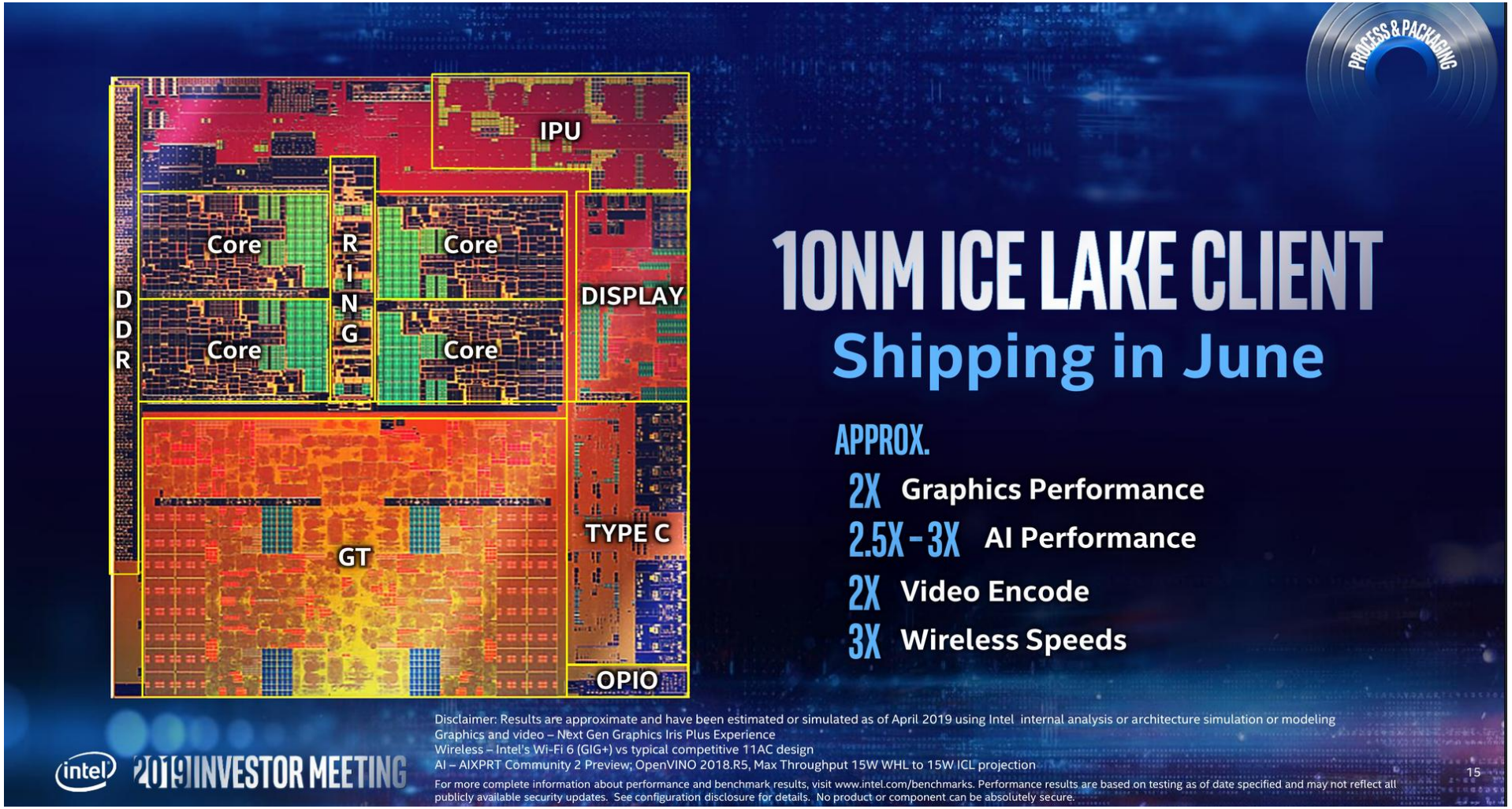
Mir Tanjidur Rahman
Instructor: Dr. Navid Asadi Zanjani
For Physical Inspection and AttacKs on ElectronicS (PHIKS)

Pix2Net Software

- ✓ A software developed by Micronet Solution Inc for automated reverse engineering (RE). (Link)
- ✓ All the companies like TechInsight have their own automated software
- ✓ Core services of the software like Pix2Net is :

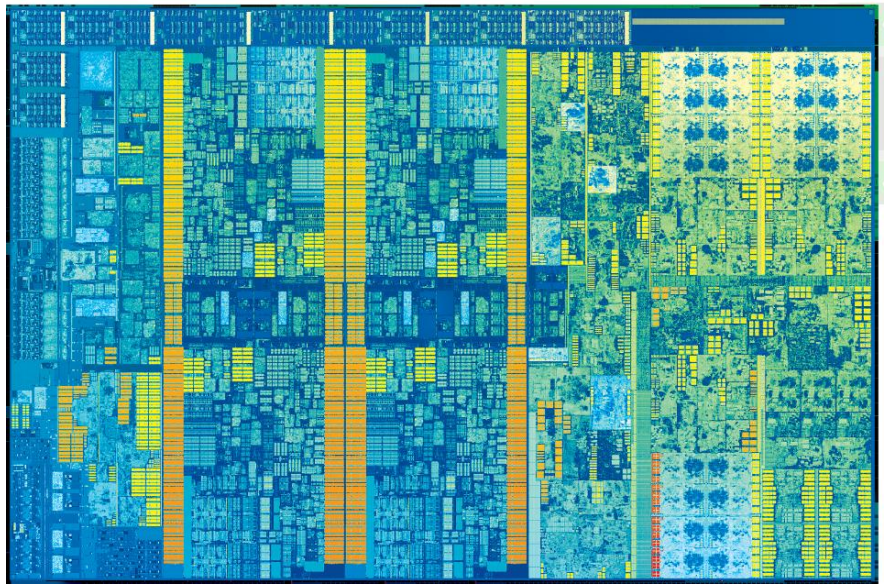
- **Reverse engineering**: from physical die to netlist and functional model extraction process. Such analysis used for failure analysis, security assessments, electrical device evaluation, electrical or environmental effect analysis, micro code analysis etc.
- **Trusted design assessment**: Hardware Trojan detection through comparing the GDSII file of trusted design and extracted design, counterfeit chip detection, anti temper circuit design, backdoor rouge circuit detection (3PIP analysis) etc.
- **Electronics and IC patent infringement assessment**: Analysis of competitor chip design for patent infringement assessment through RE.

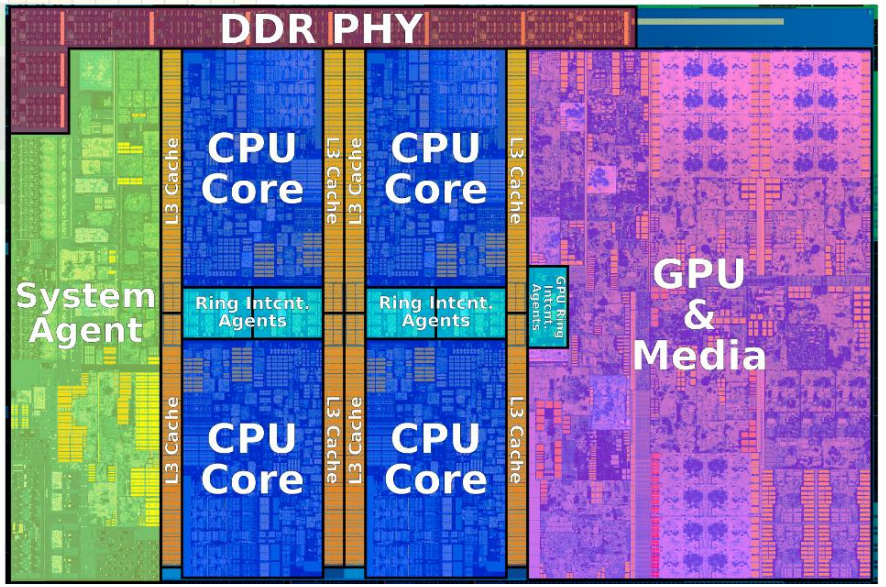
New CPU/SoCs etc.

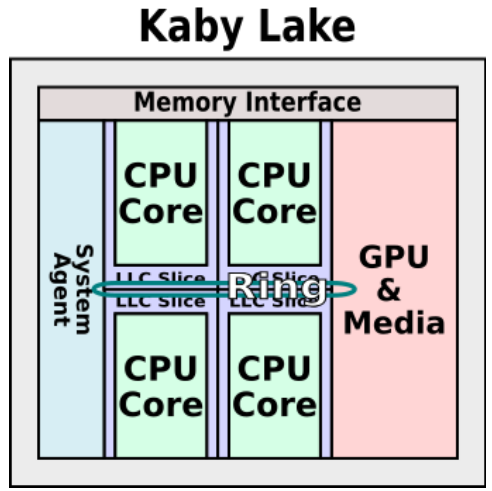


https://fuse.wikichip.org/news/1711/intel-discloses-9th-gen-core-refreshes-core-x-and-reintroduces-stim/

Ips in SoCs



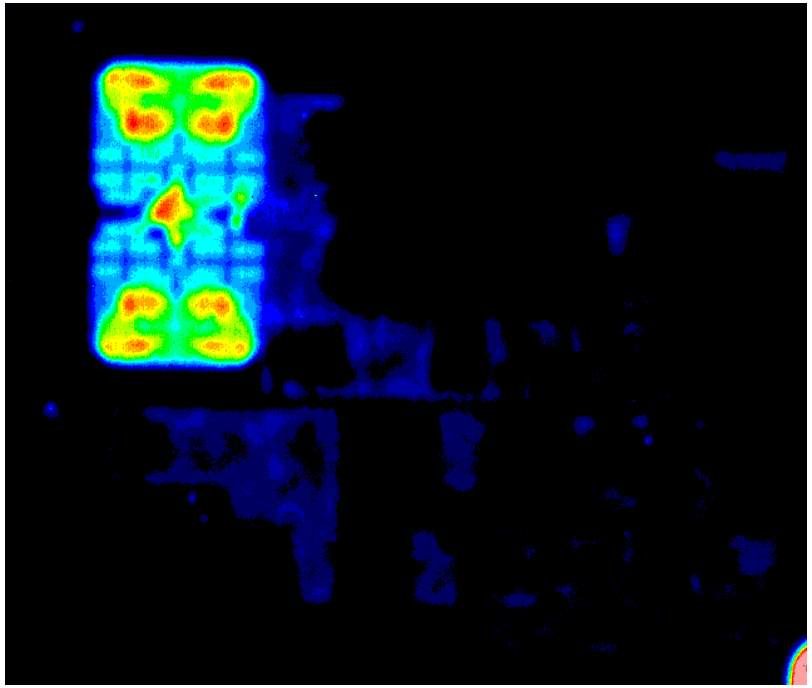


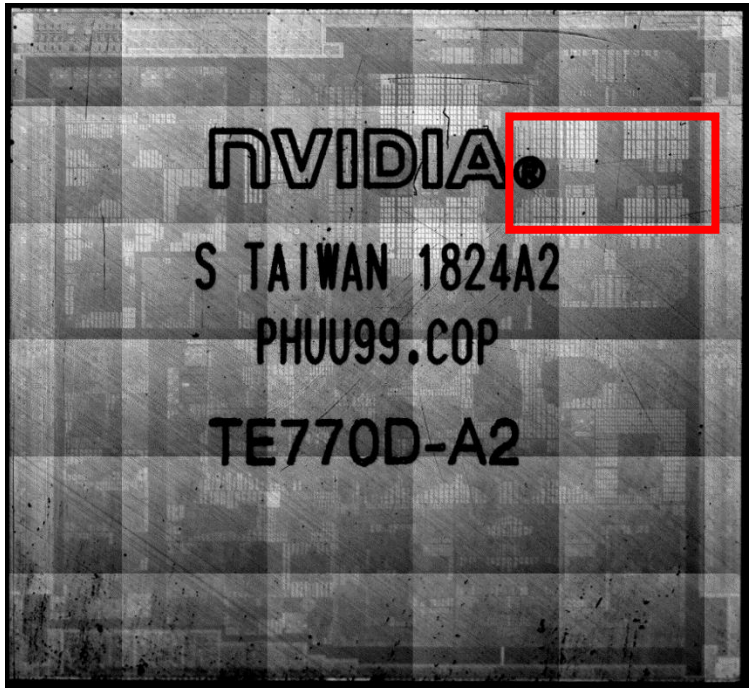


- Memory location, BUS, cache, etc. can be distinguished from repetitive pattern in the device
- Logic areas are highly irregular areas and easily differentiable from memory or cache.

https://fuse.wikichip.org/news/1711/intel-discloses-9th-gen-core-refreshes-core-x-and-reintroduces-stim/

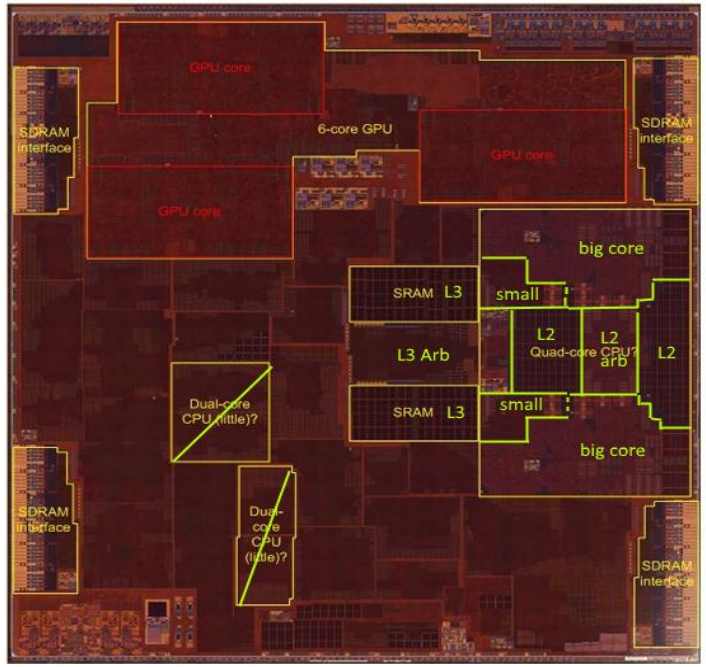
ARM Core Detection





Work Completed by Dhwani Mehta for PAINE Wrokshop

Hardware IPs implemented
In Apple A10 Quadcore SoC

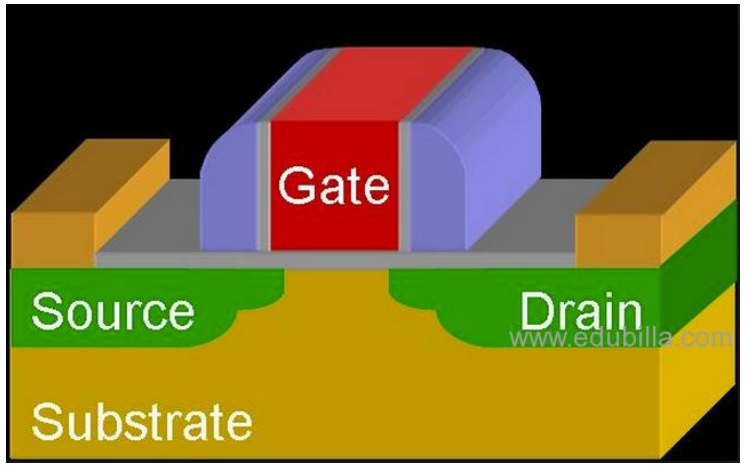


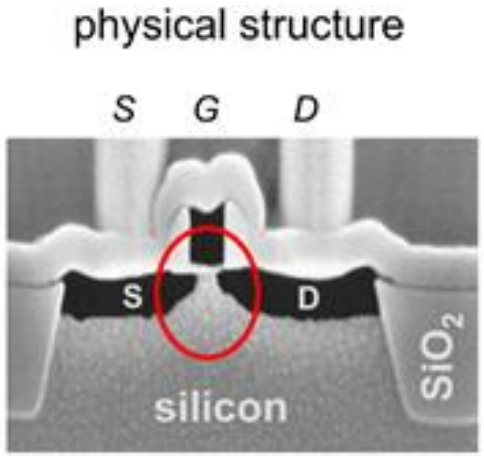
- TSMC's **16 nm** FinFET
- **3.3 billion** transistors
- Die size: 125 mm^2

@Chipworks

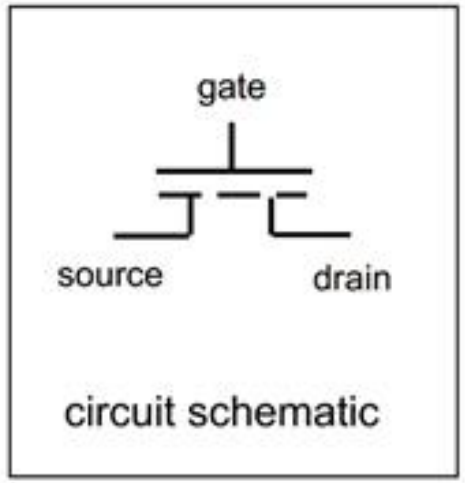
- CORE, cache, registers can also be identified from photonic emission analysis; but that's a different story we will learn later in the course

VLSI & Fabrication Process: Planer MOSFET

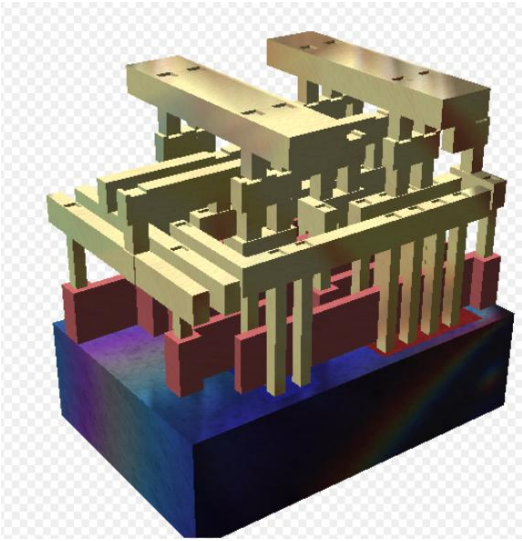


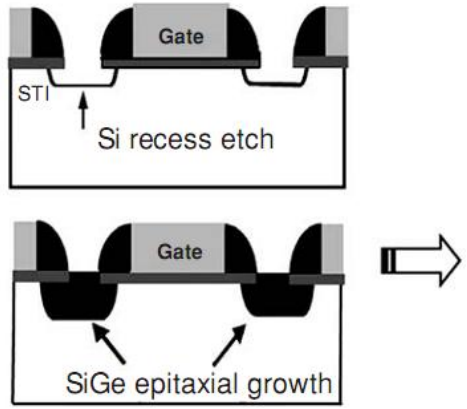


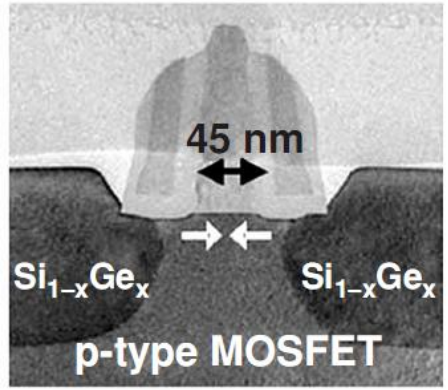
(Texas Instruments, 1997)



Planner MOSFET



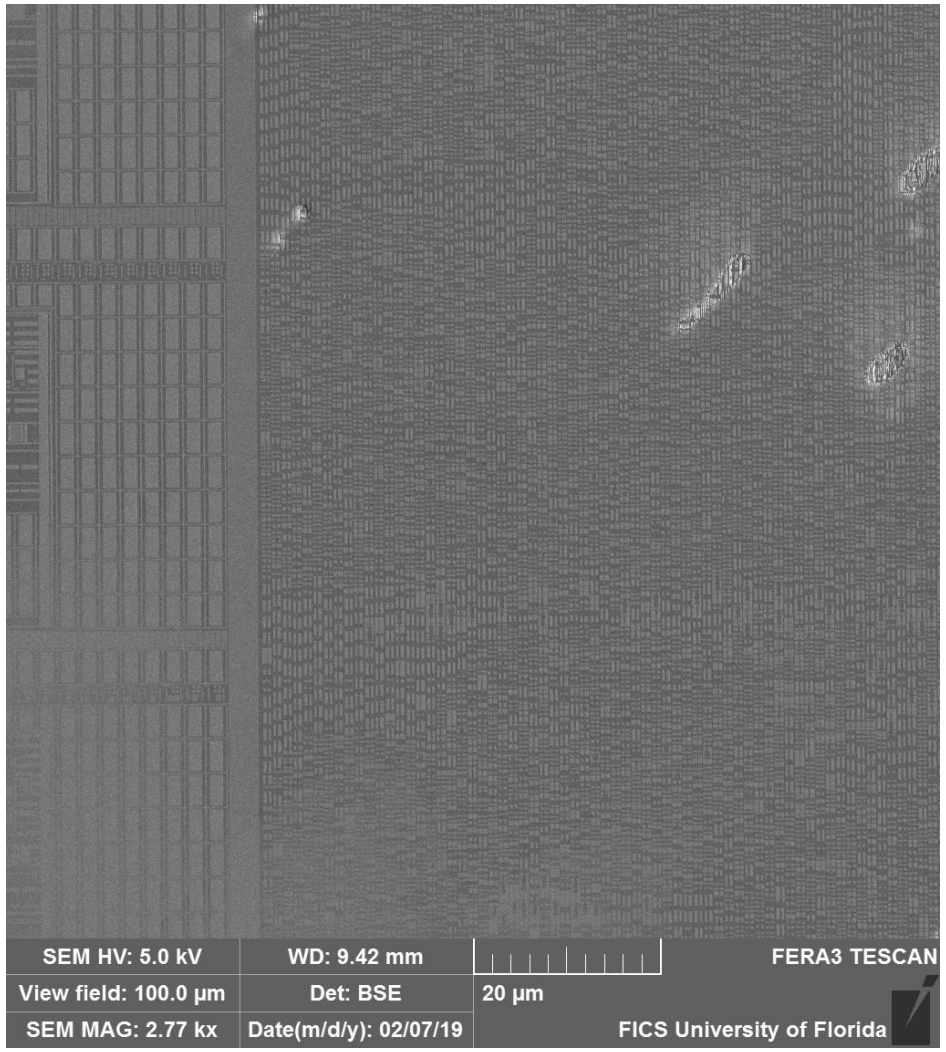


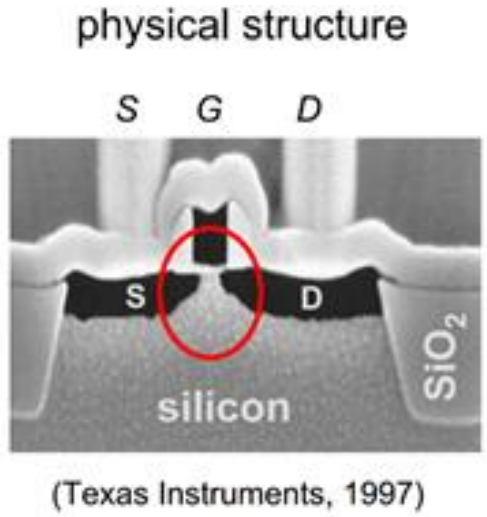


Equal width p and n-type MOSFET

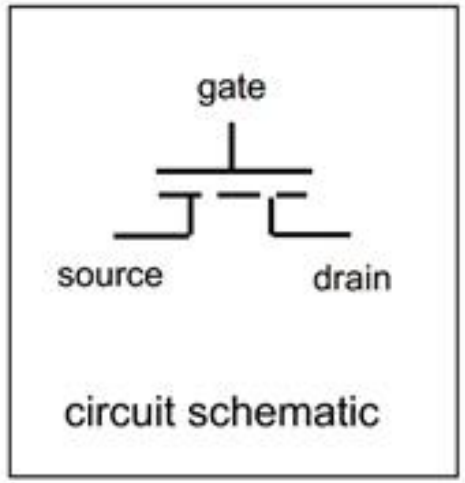
Watch List: 1. https://www.youtube.com/watch?v=d9SWNLZvA8g
2. https://www.youtube.com/watch?v=uWHxggc-O94

VLSI & Fabrication Process: Planer MOSFET

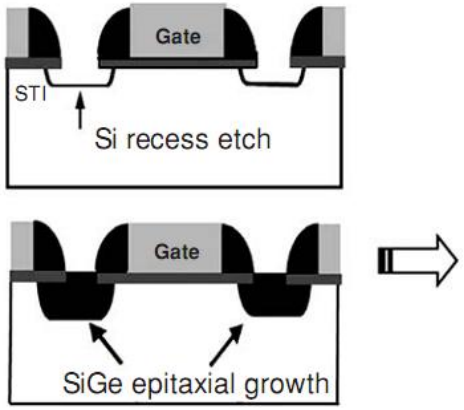


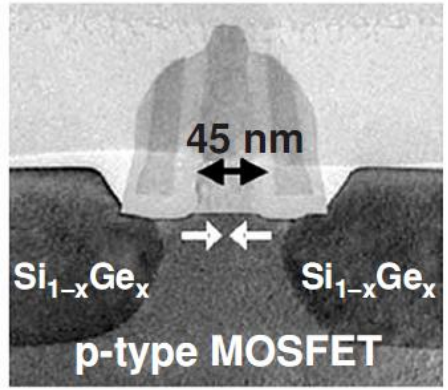


(Texas Instruments, 1997)



Planner MOSFET

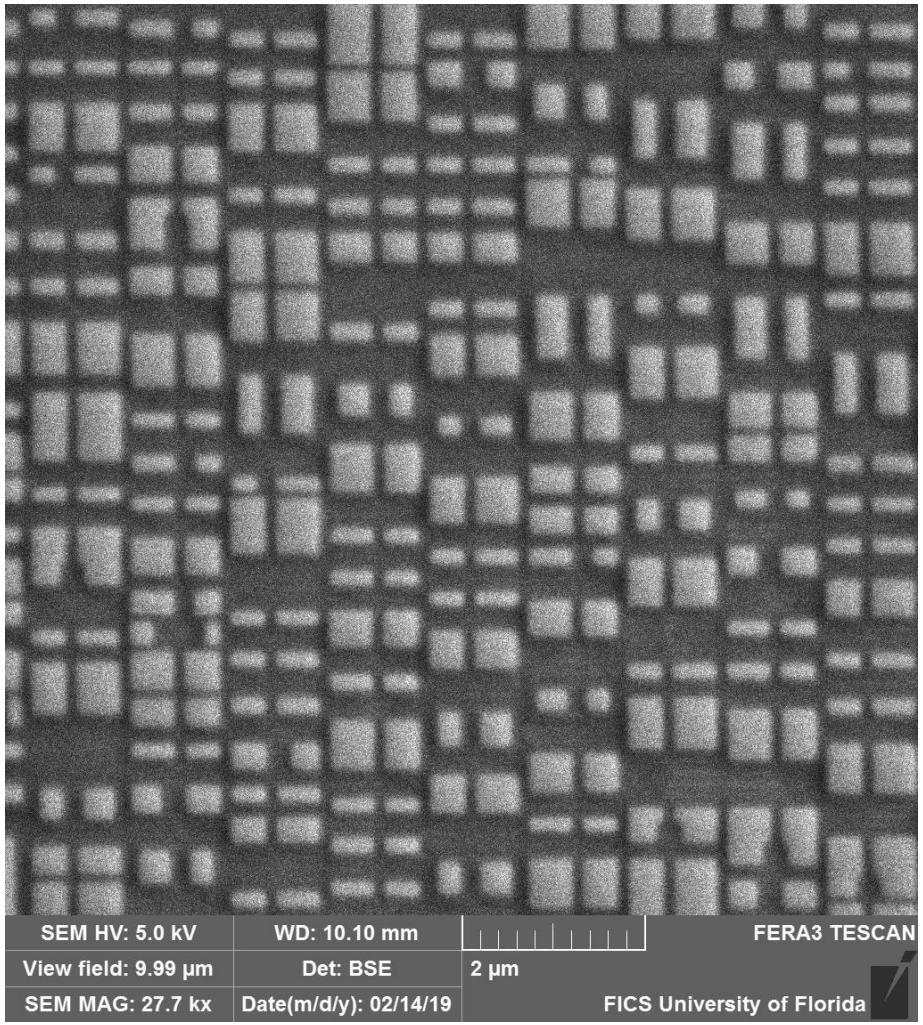


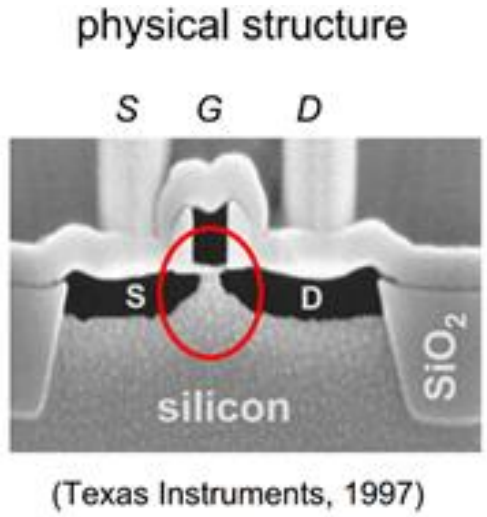


Equal width p and n-type MOSFET

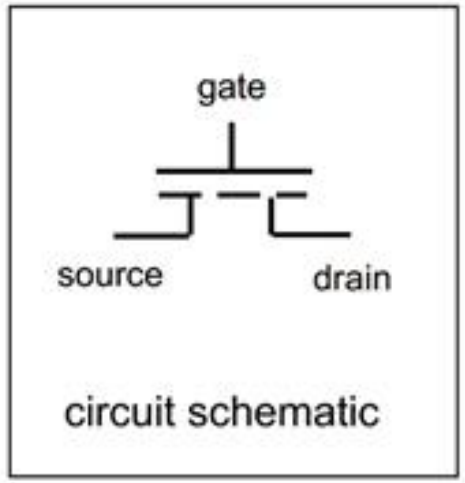
https://www.extremetech.com/extreme/191996-zoom-into-a-computer-chip-watch-this-video-to-fully-appreciate-just-how-magical-modern-microchips-are

VLSI & Fabrication Process: Planer MOSFET

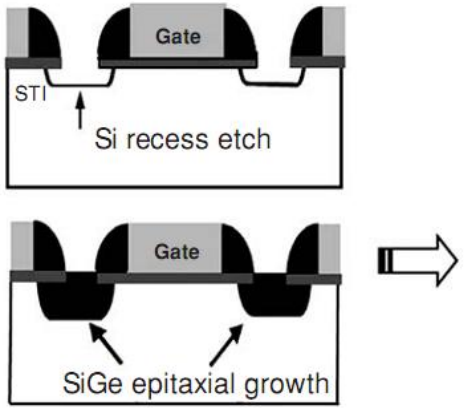


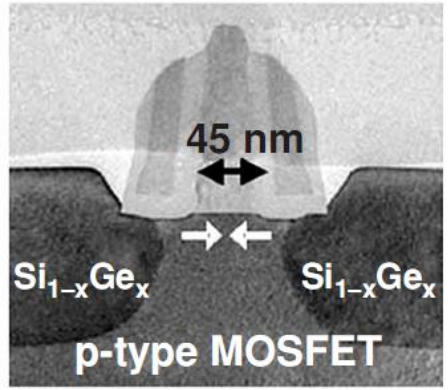


(Texas Instruments, 1997)



Planner MOSFET

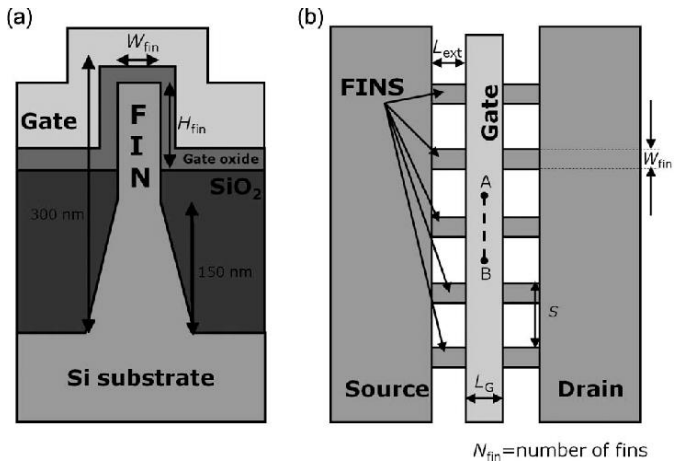




Equal width p and n-type MOSFET

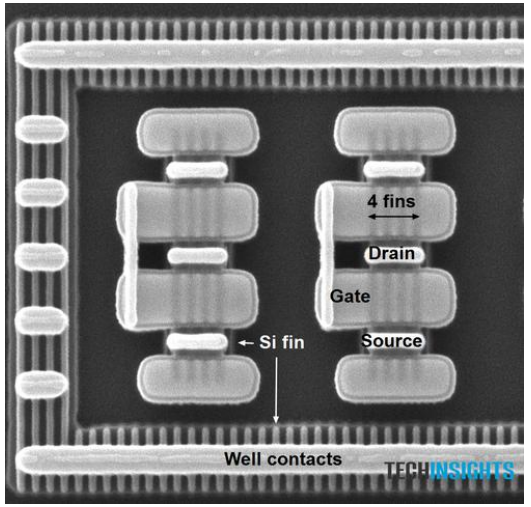
https://www.extremetech.com/extreme/191996-zoom-into-a-computer-chip-watch-this-video-to-fully-appreciate-just-how-magical-modern-microchips-are

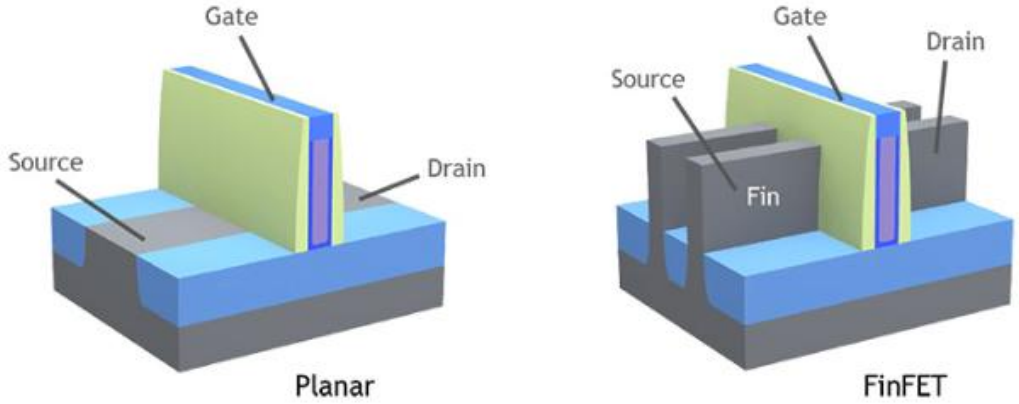
VLSI & Fabrication Process: FinFET MOSFET



Cross section and top view of FINFET

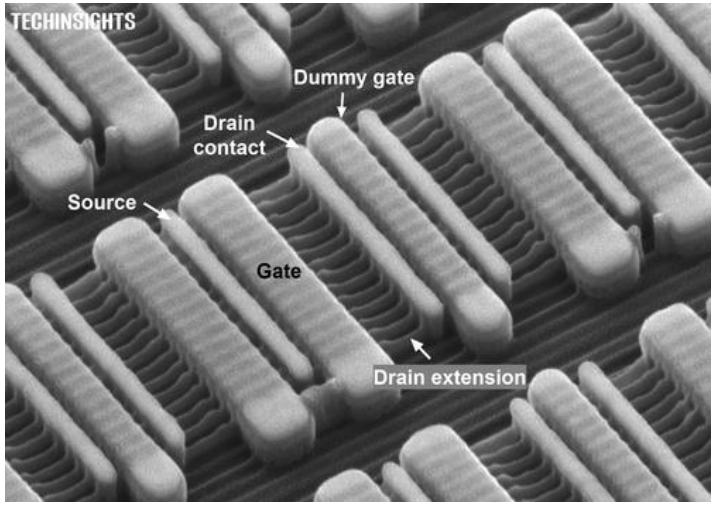
Source: Time-dependent dielectric breakdown on subnanometer EOT nMOS Finfet





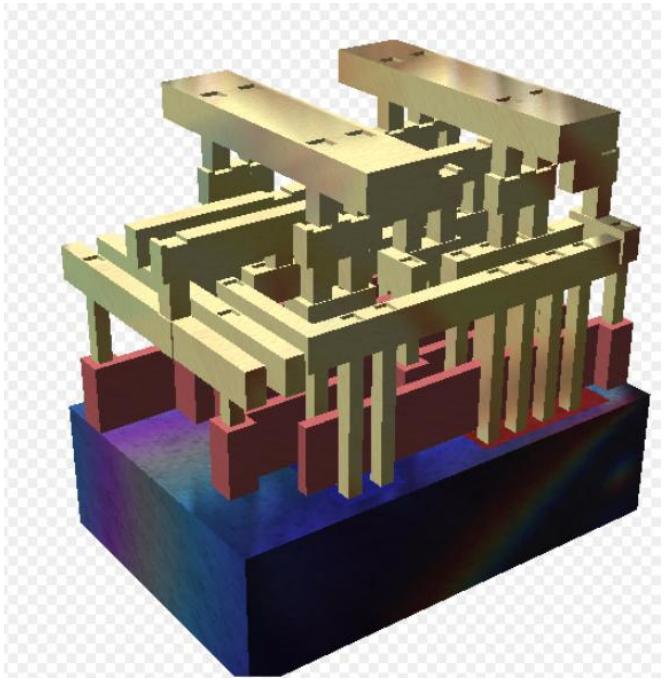
Planner MOSFET Vs FINFET

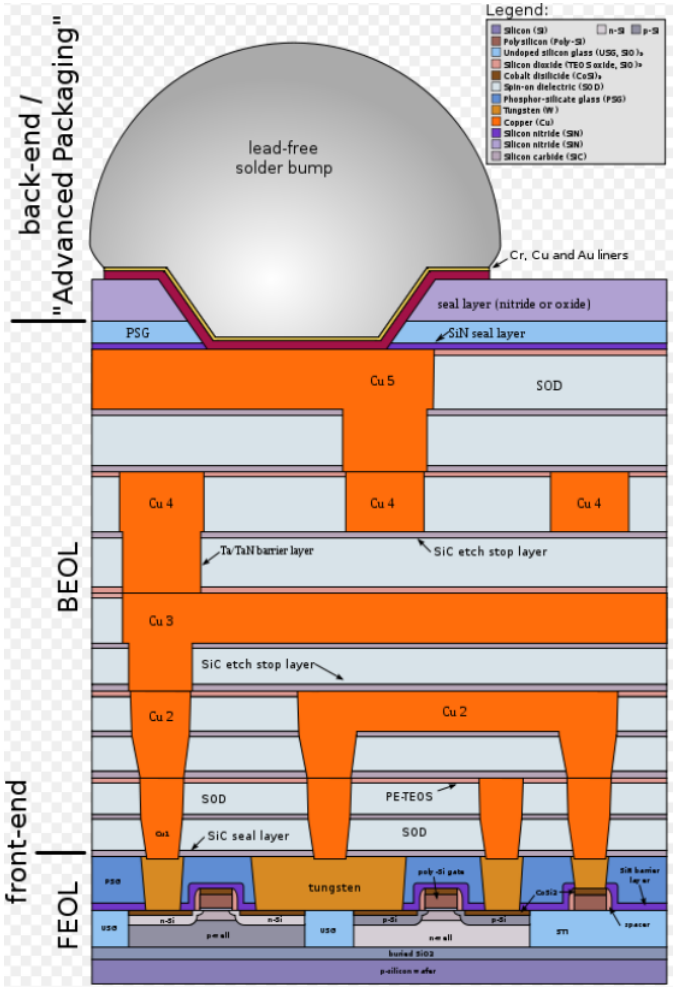
Source: https://semiengineering.com/finfet-metrology-challenges-grow/

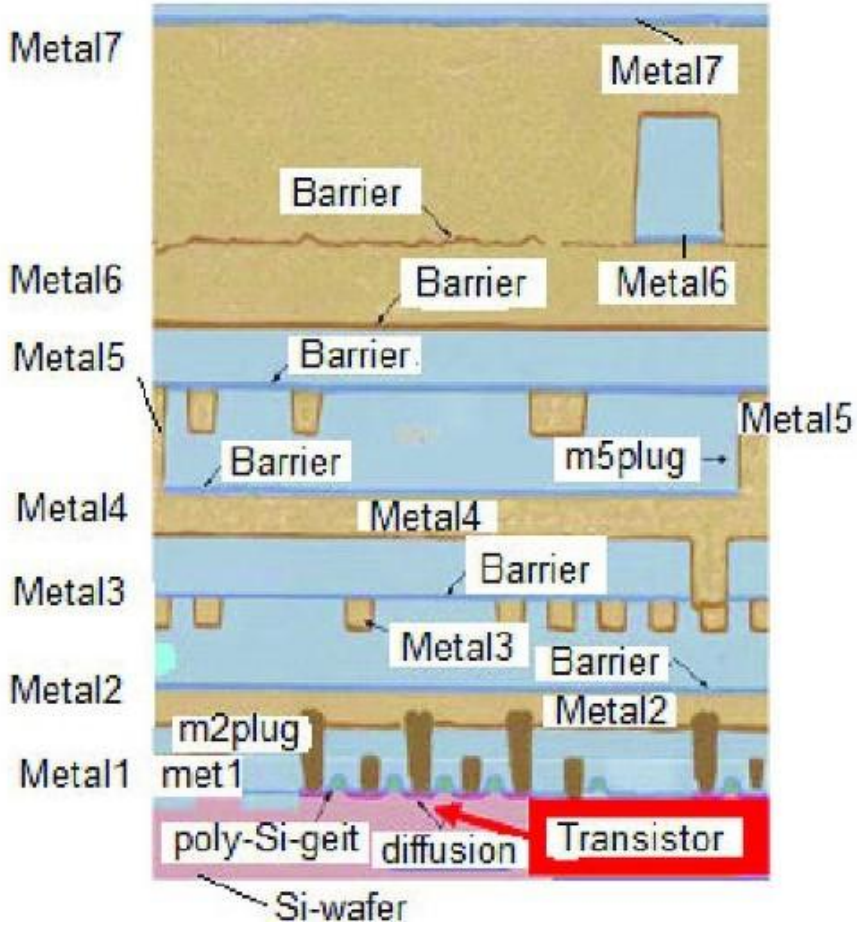


@Techinsight

VLSI & Fabrication Process: Metal Layers and Vias





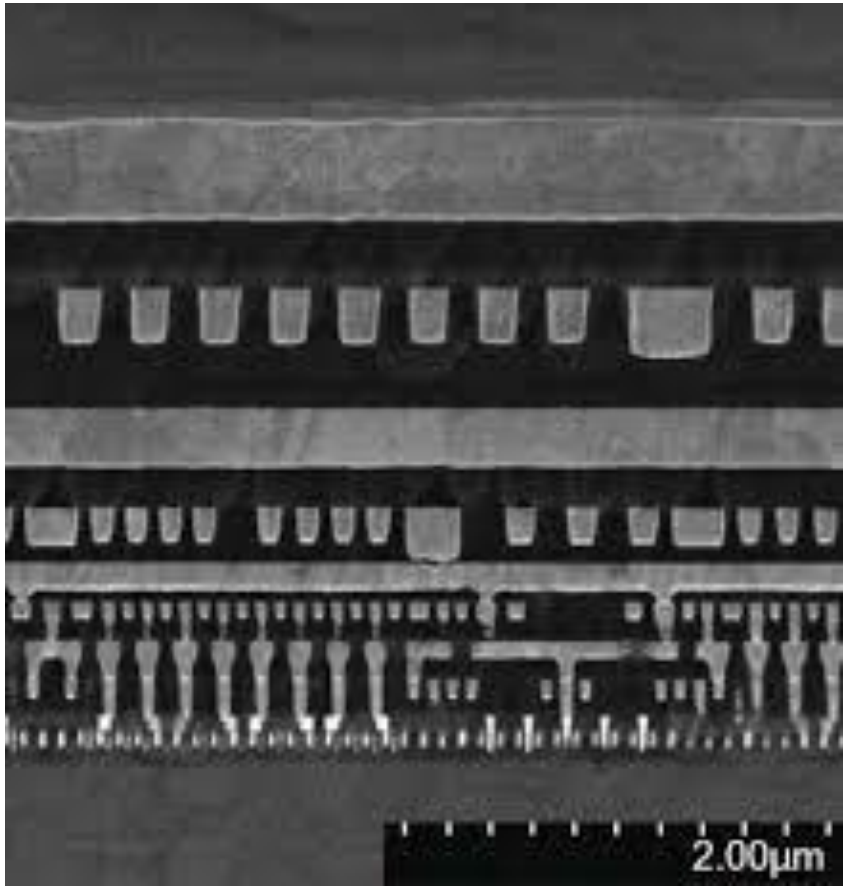


- Model cross section of ICs

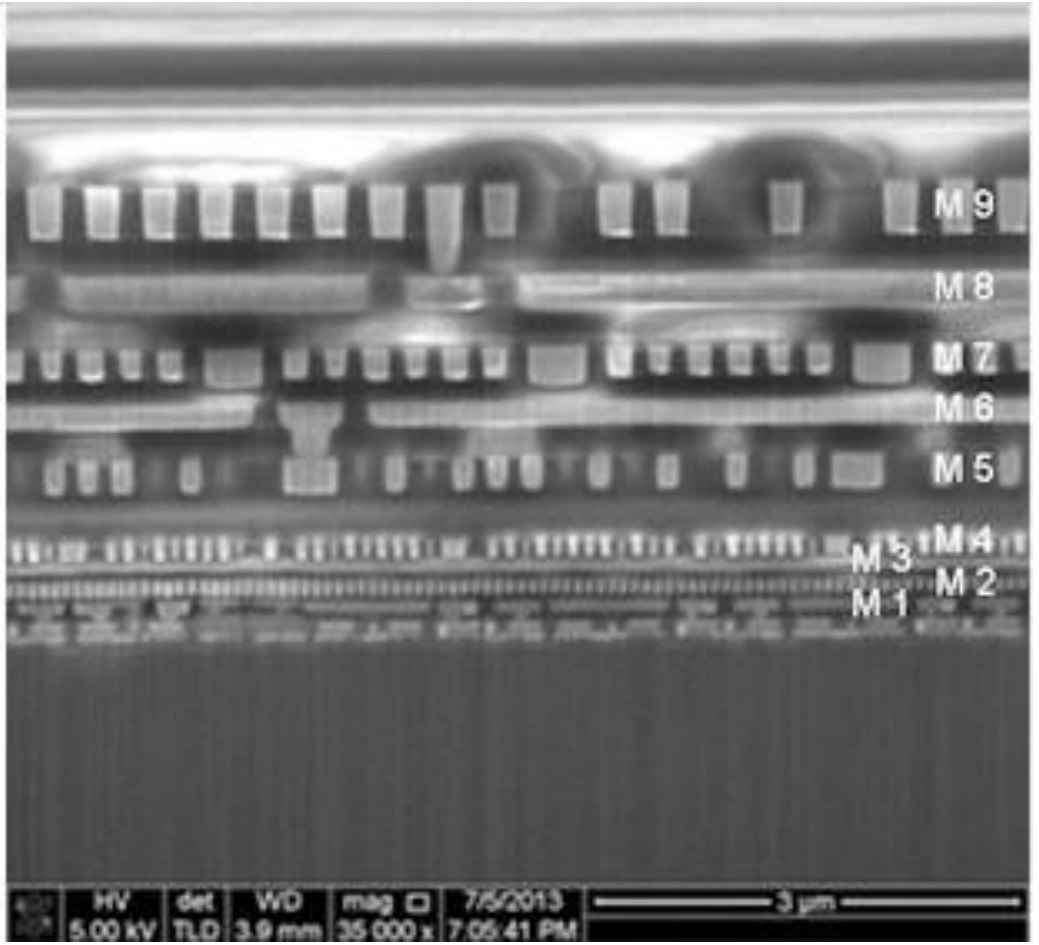
Different layers in Ics, transistors placed at the bottom of metal layers

Watch List: 1. https://www.youtube.com/watch?v=d9SWNLZvA8g
2. https://www.youtube.com/watch?v=uWHxggc-O94

VLSI & Fabrication Process: Metal Layers and Vias



SEM image of different metal layers and transistors



Different metal layers in the SEM image cross section

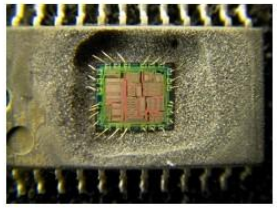
http://www.ma-tek.com/en-global/services/index/material/FIB

Reverse Engineering Workflow and the Outcome

Reverse Engineering Steps

Depacakging
- Frontside
- Backside

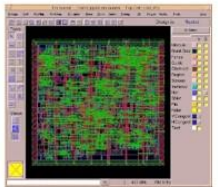
Clean & Prep
(Planarize)



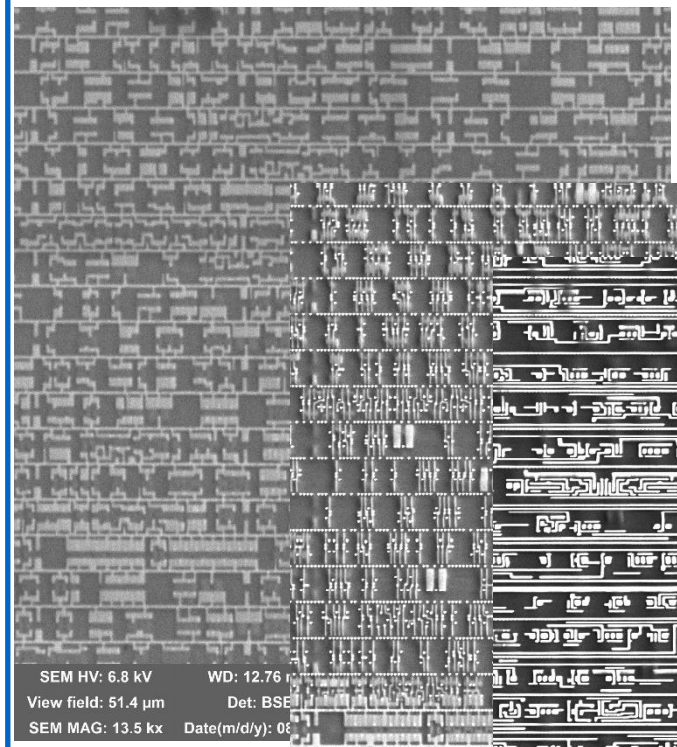
Imaging
- SEM/ Optical

Delayering
- Plasma/FIB etching
- Wet etching

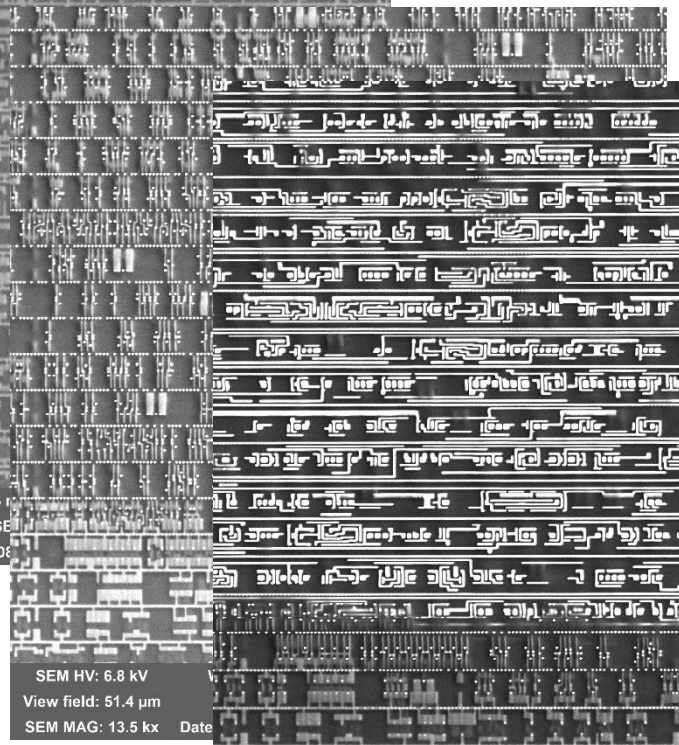
Extract Netlist
- Pix2Net
- Chipjuice



Outcome of Process



Active layer

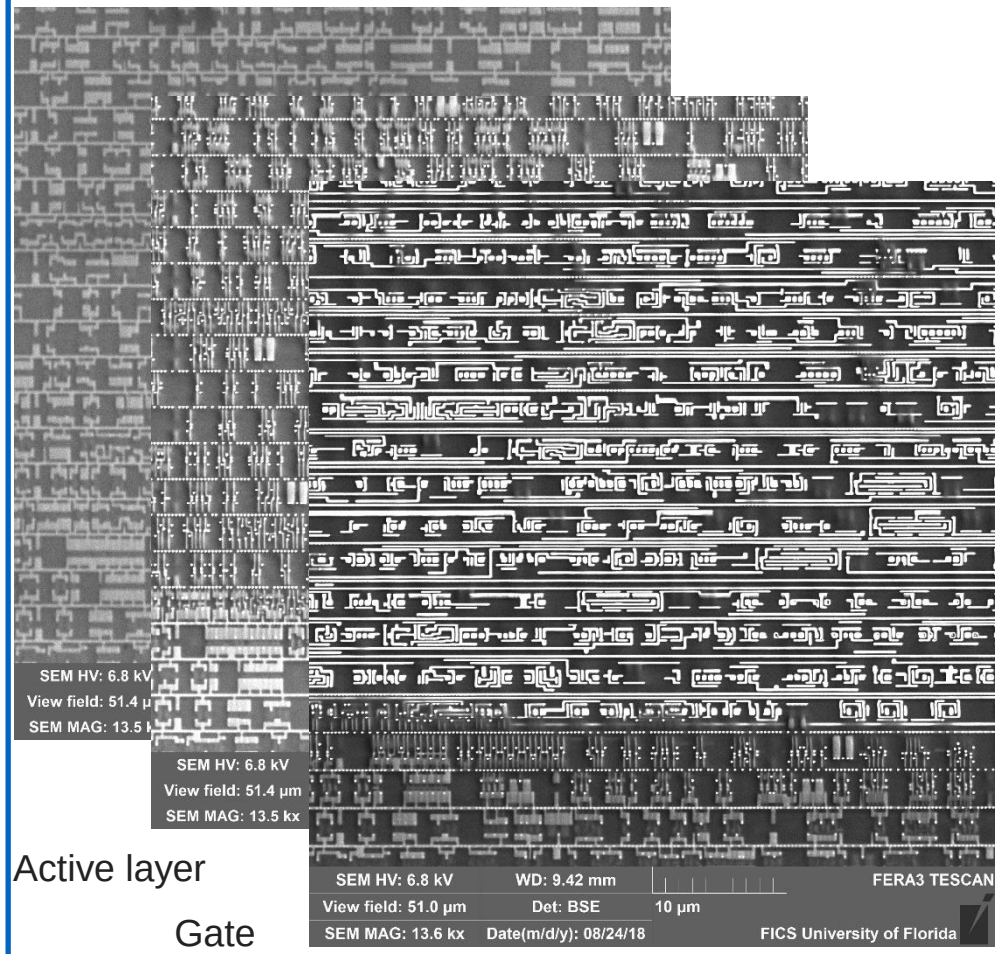


Gate

Metal layers

Understanding the Connection in SoCs

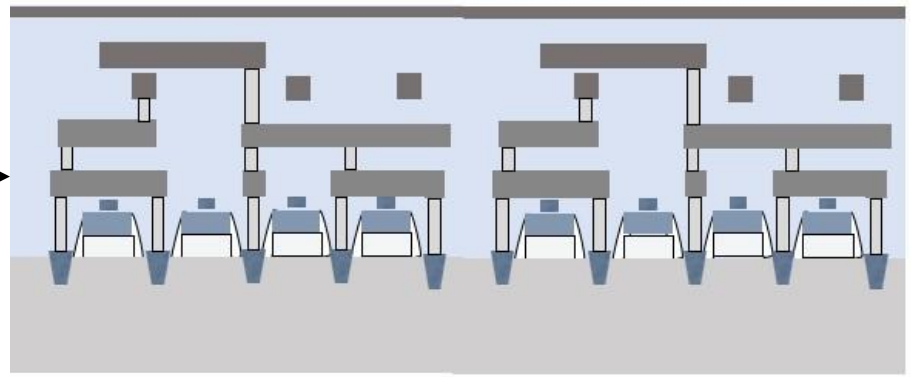
Outcome of Process



Active layer

Gate

Metal layers

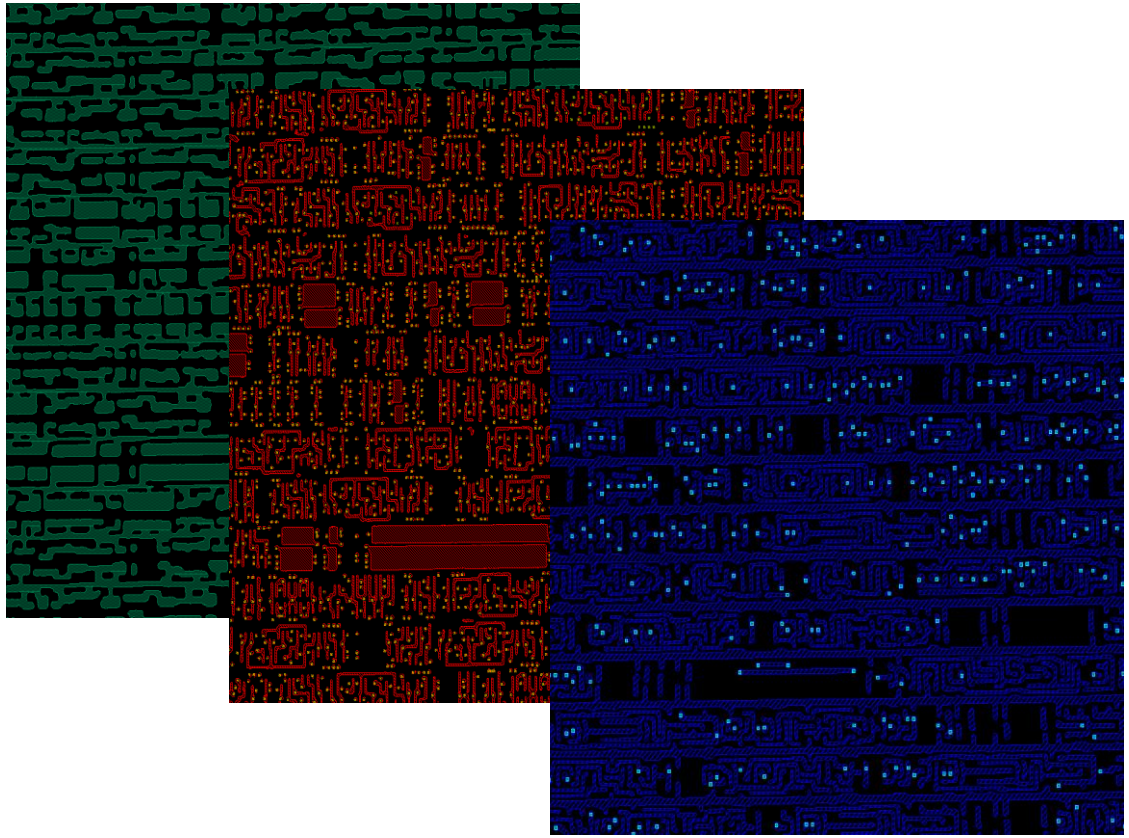


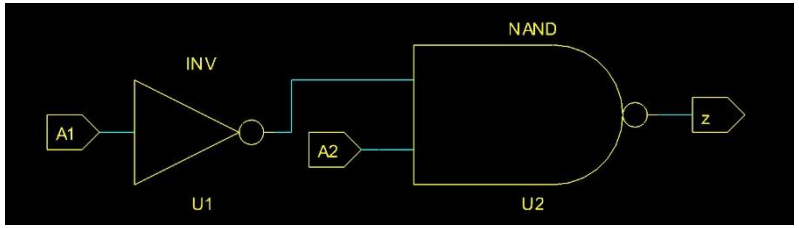
After overlaying, the layers should be aligned at the same way, they were aligned in the device. Otherwise the connection diagram will be wrong.

Challenges of Netlist Extraction Software

Challenges of Reverse Engineering

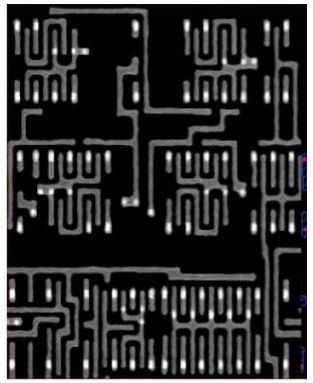
- Outcome is not machine readable
- Apply computer vision for reading the connection
- Detecting each transistor can not be manual
- Variation in gates and devices
- Functionality of each gate extraction
- Convert the outcome into GDSII or Verilog or functional verification format

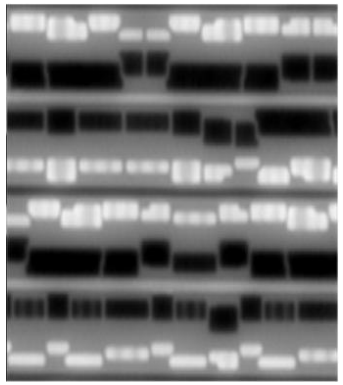


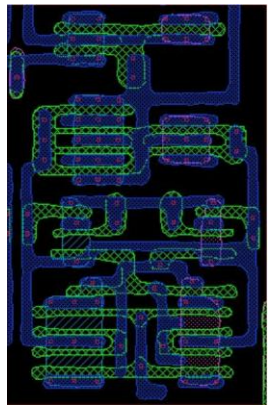


Workflow of Netlist Reverse Engineering

Delayering Interconnects → Diffusion Implant Extraction → Stich and alignment of layers → Polygon Extraction

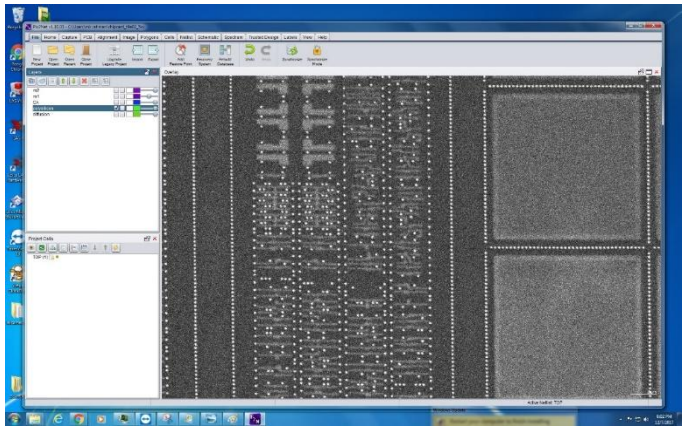




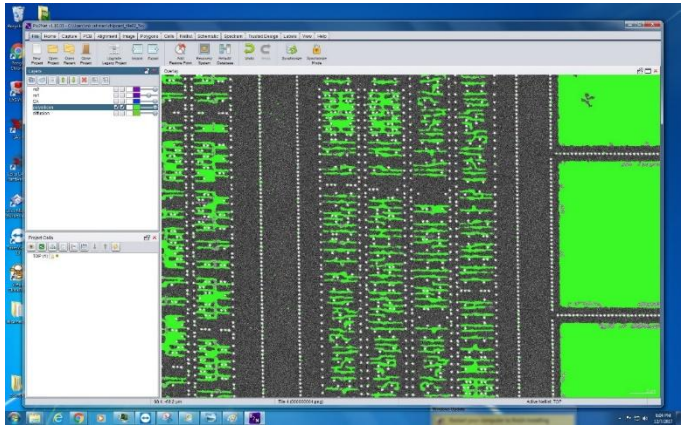


Polygon Extraction

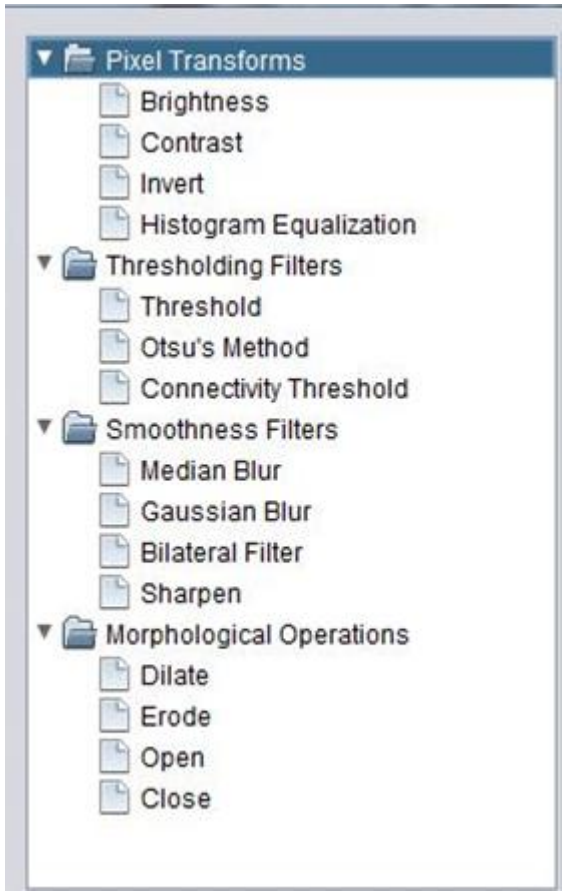
Converts the SEM image into machine readable vector with the help of image processing and computer vision



SEM image



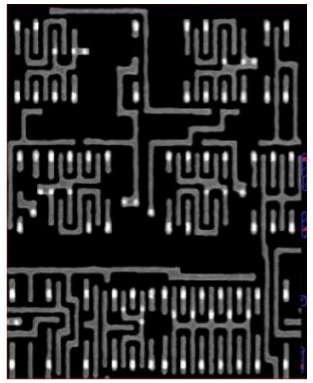
Polygon Extracted image

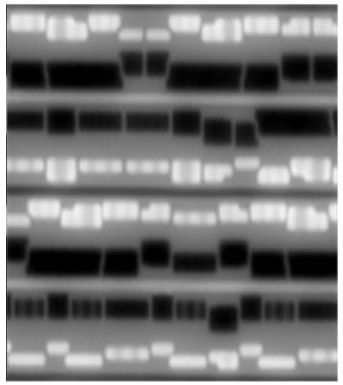


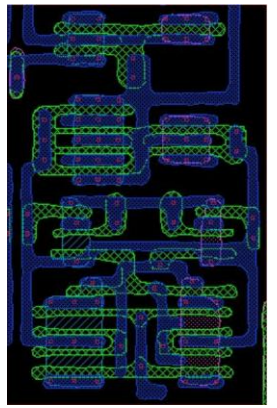
- Accuracy of polygon extraction significantly effect the accuracy and effort required for circuit extraction
- Several in-built filters are available in Pix2Net software to improve the image quality

Workflow of Netlist Reverse Engineering

Delayering Interconnects → Diffusion Implant Extraction → Stich and alignment of layers → Polygon Extraction → Extract Library Cell Extraction







Workflow of Netlist Reverse Engineering

Extract Library Cell Extraction

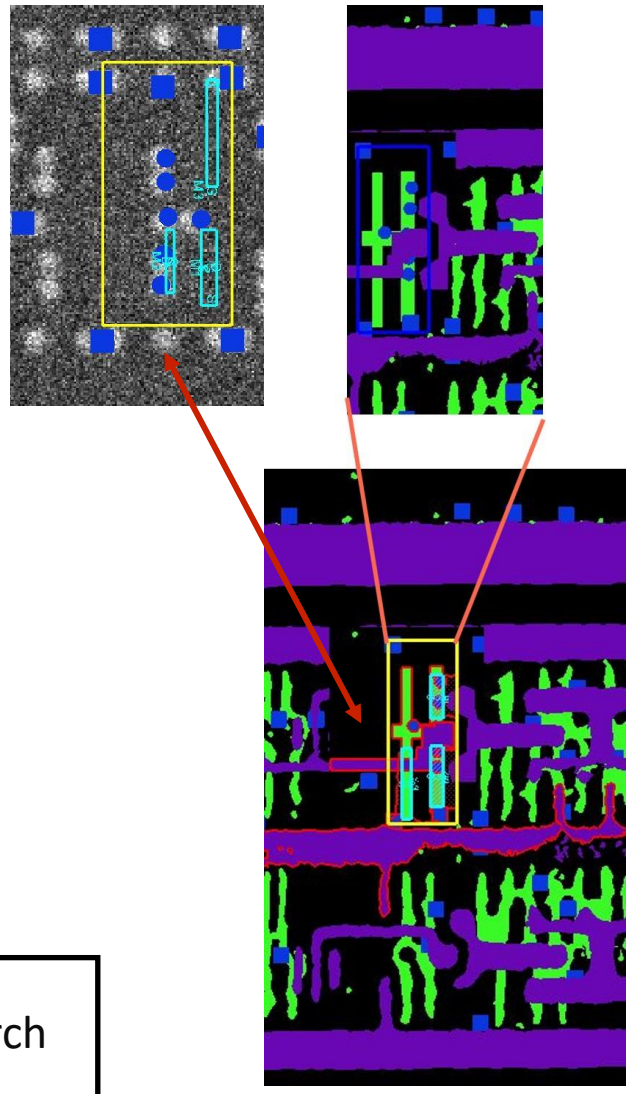
Identify Transistor at polysilicon layer

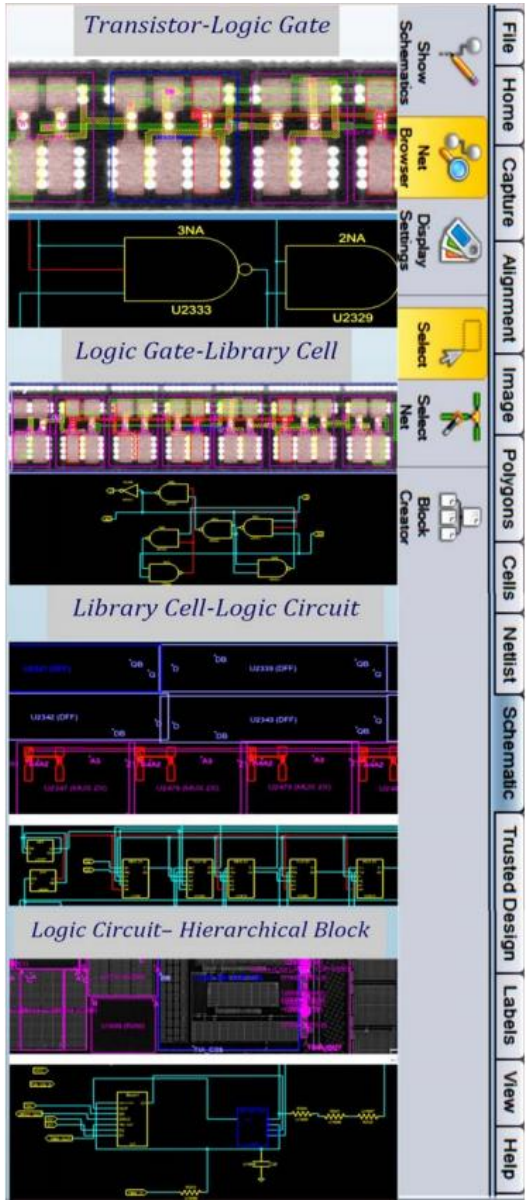
Identify I/O Port

Netlist Extraction

Truth Table and Verilog Code Extraction

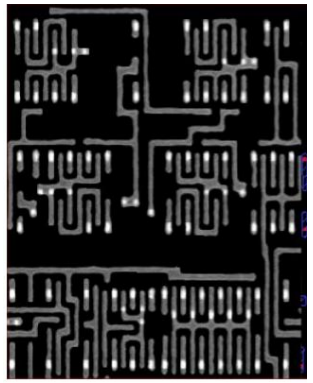
Instance Search



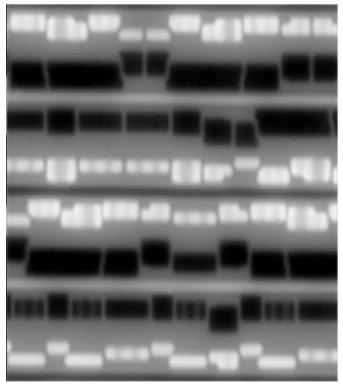


Workflow of Netlist Reverse Engineering

Delayering Interconnects

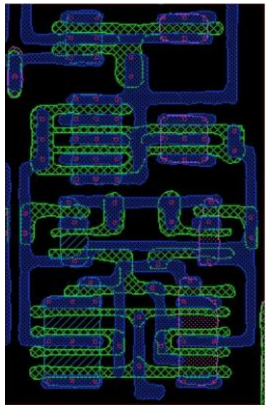


Diffusion Implant Extraction



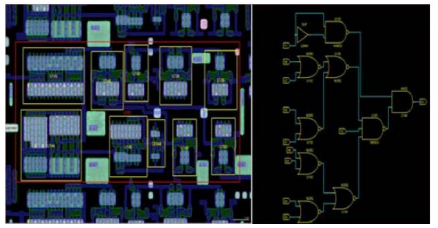
Stich and alignment of layers

Polygon Extraction

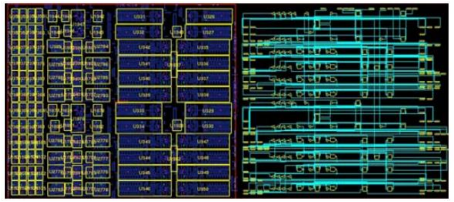


Extract Library Cell Extraction

Netlist Schematic Generation



Circuit Block Extraction



Logic Gate Structure

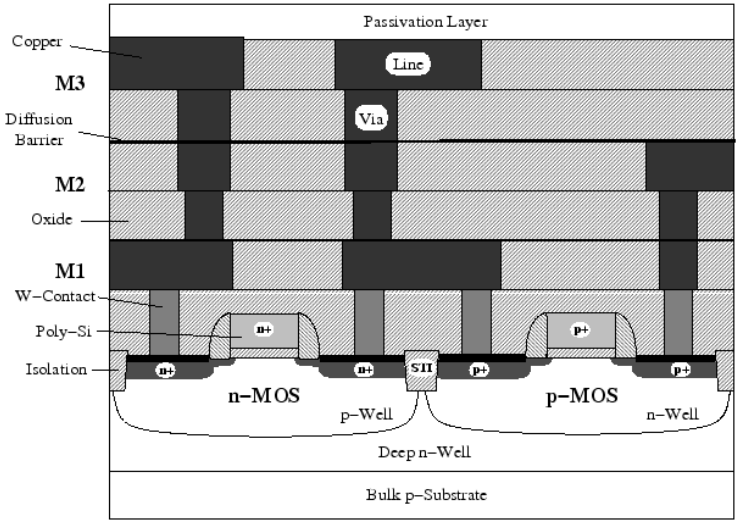
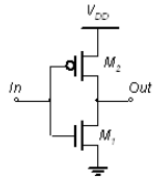
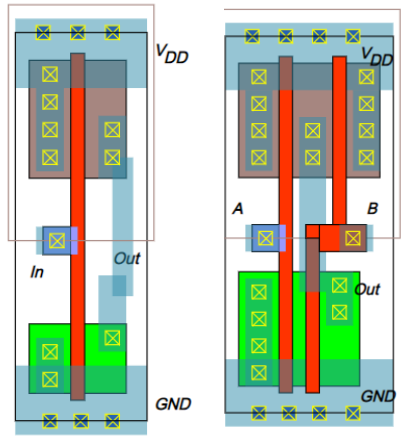


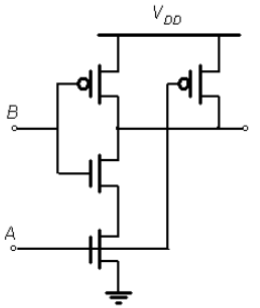
Figure 1.1: Schematic cross-section of a final CMOS integrated circuit with an interconnect structure of three metal layers (M1 - M3).

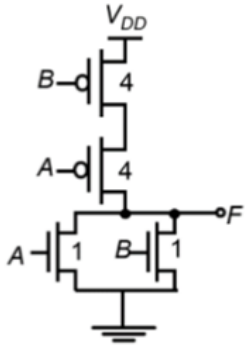


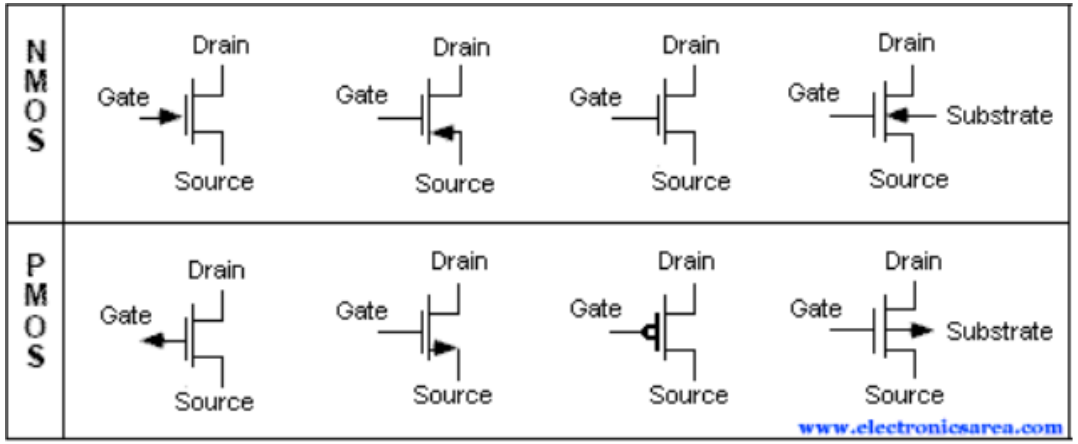
Inverter circuit



2-input NAND gate

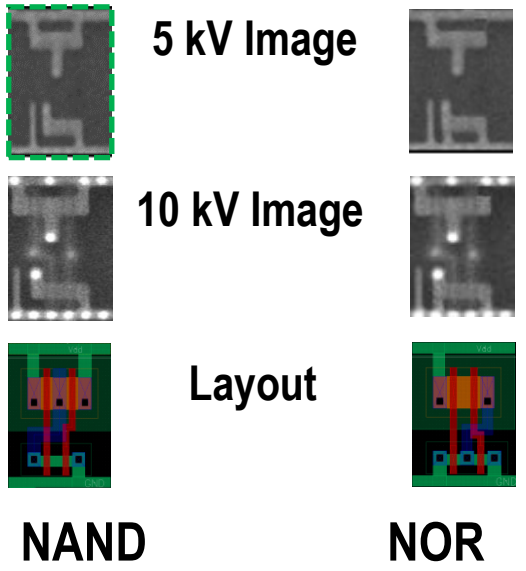






NMOS and PMOS transistor Symbols

Image Quality and Trojan Scanner



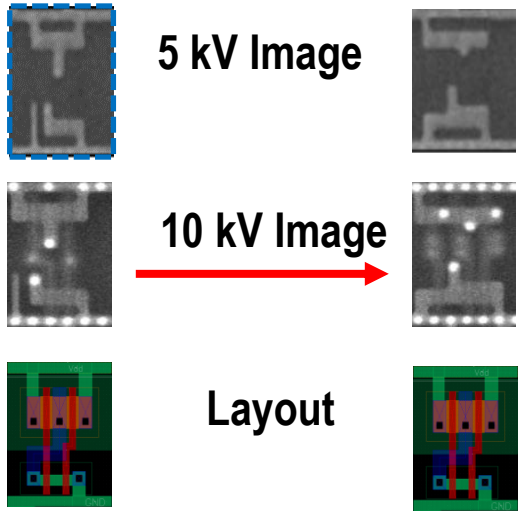
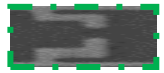
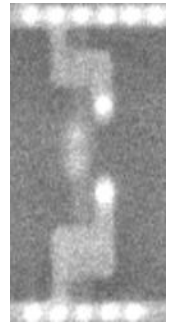
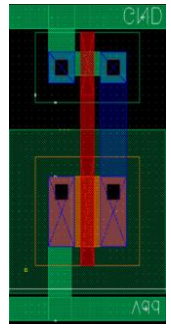


Image Quality and Trojan Scanner

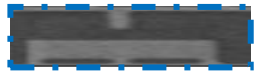


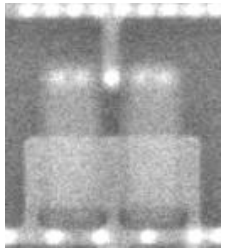


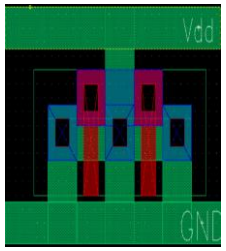


5 kV Image 10 kV Image Layout

Inverter



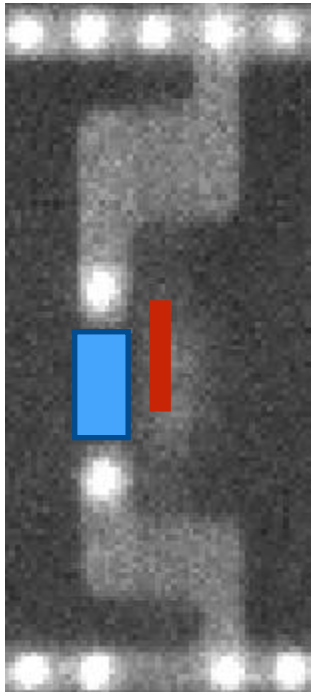




5 kV Image 10 kV Image Layout

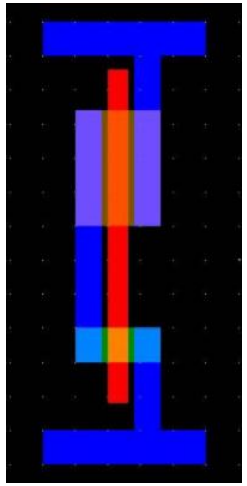
MOS Capacitor

Manual RE: Logic Extraction

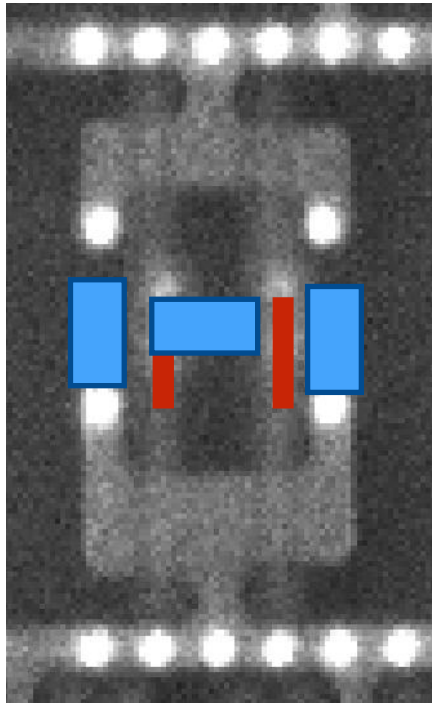


PMOS

NMOS



Inverter

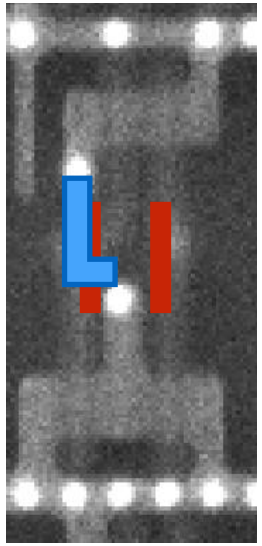


NMOS

PMOS

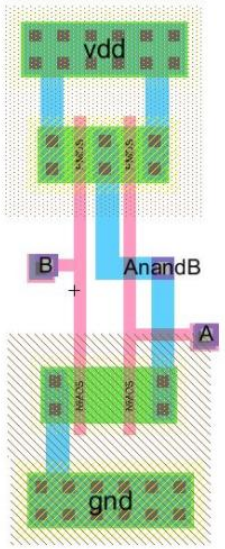
Buffer

Practice Problem



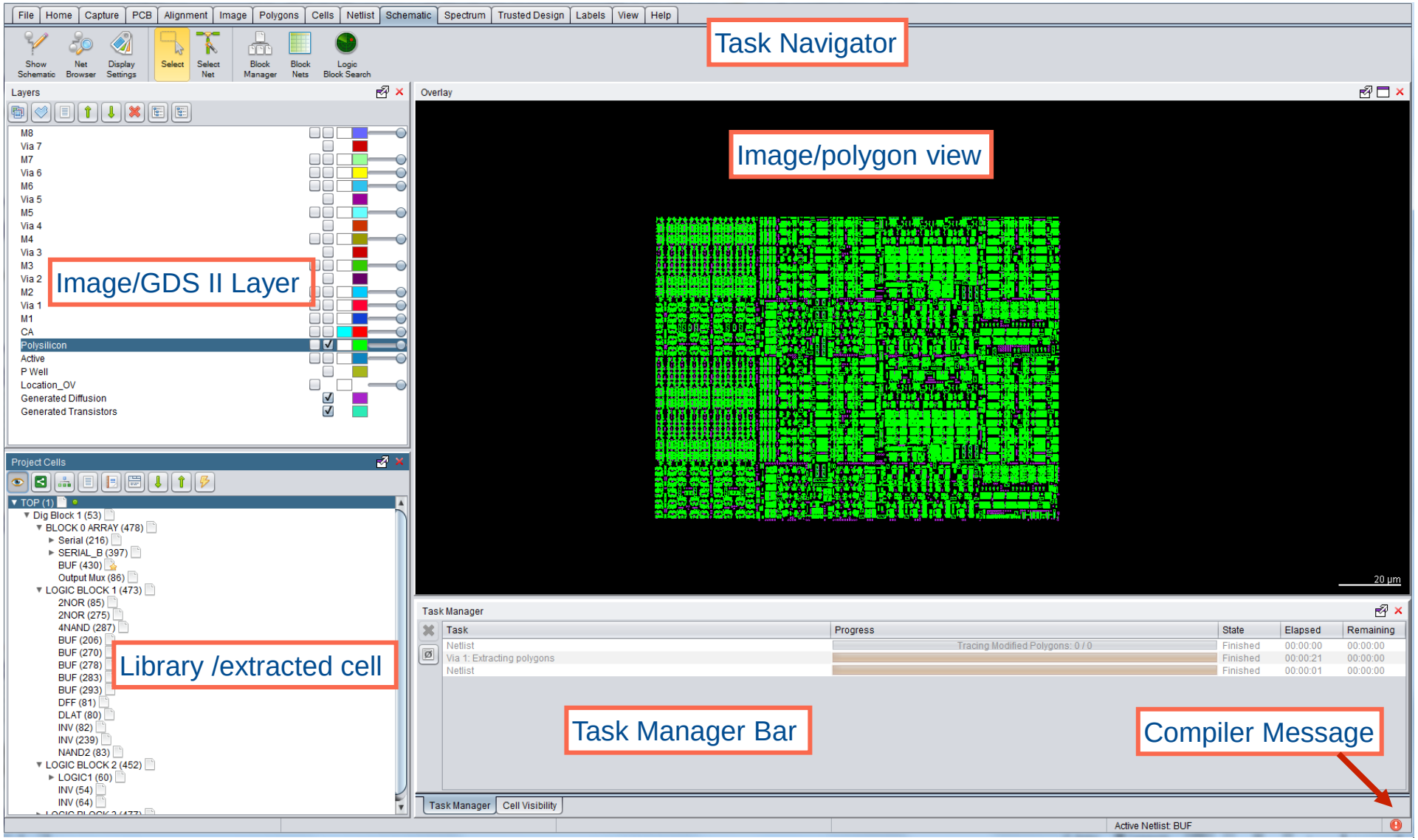
NMOS

PMOS

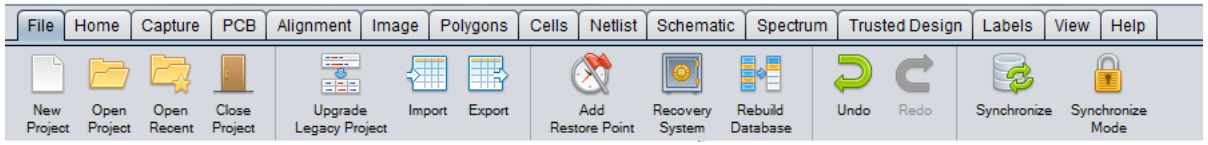


NAND

Pix2Net Layout

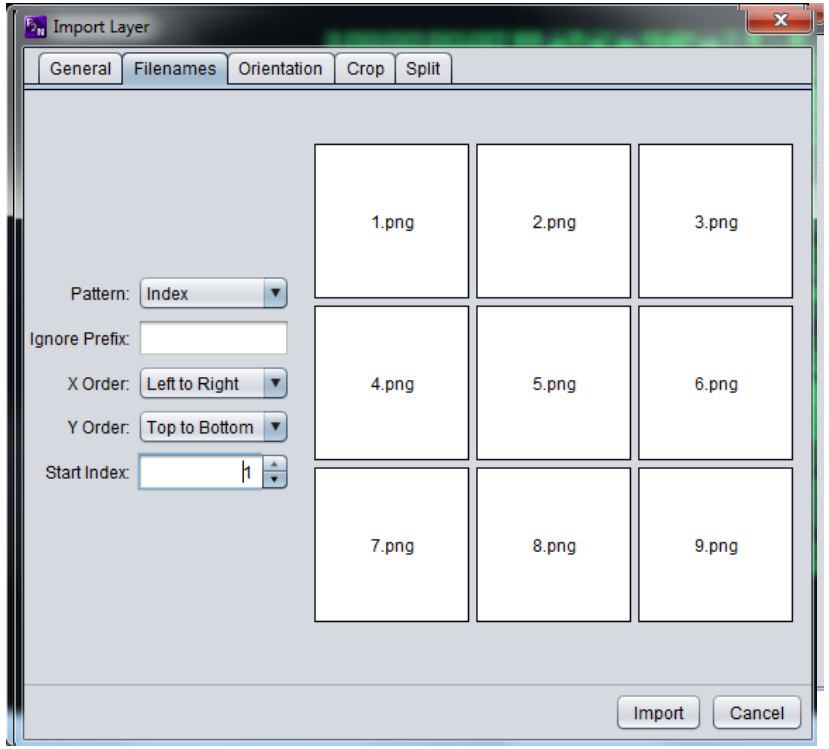


Process Flow



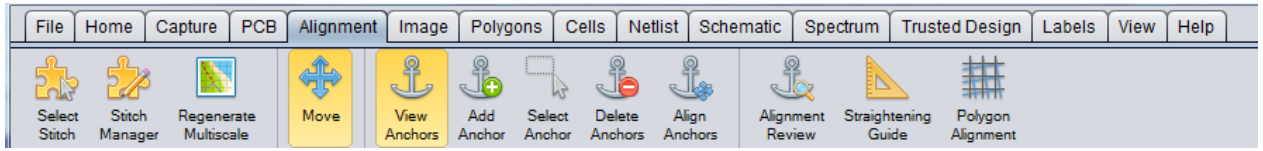
- ✓ File Tab:
  - Start a new project
  - In import icon import the image/GDS file
    - Decide single/multiple image
    - Define pixel/um
    - Define number of rows/column
    - For multiple image import place all images of same layer in a single folder and number them accordingly
  - Repeat same process for each layer
  - Provide active and p-diff or p-diff and n-diff information
  - Restore point creates a zip file for each point
  - Synchronize command synchronize the project on server
  - Upgrade legacy project

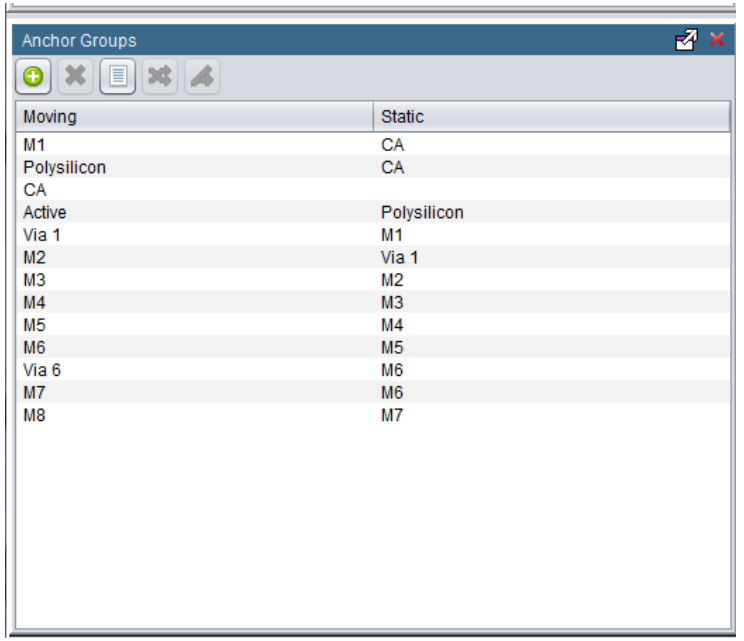
Note: For any detail information check help tab



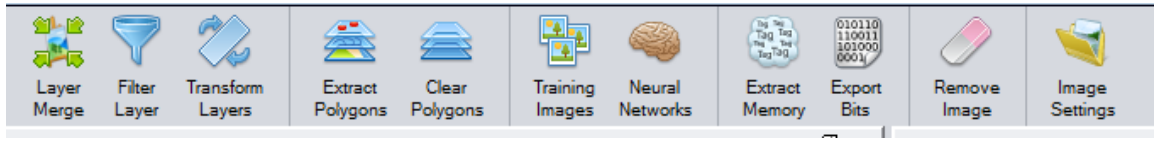
Process Flow

- ✓ Alignment Tab:
  - Use stich/stich manager
  - Move command used for manual alignment
  - Add anchor define the positions that are aligned t ogether
  - Moving and static layer group define the reference layer and moving layer



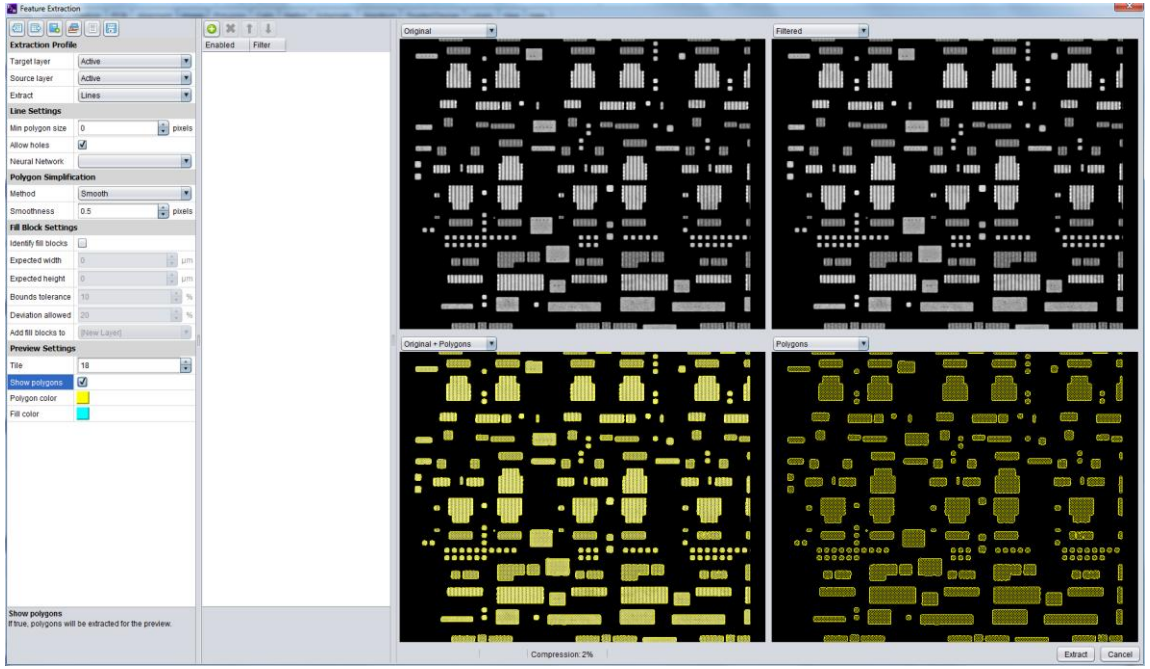


Process Flow



✓ Image Tab: Extracts polygon

- Filtering and edge detection, and neural network is available for polygon extraction
- Use Extract Polygon command
- Filters are used for extraction
- Target and source layer, vias/lines must be defined
- Clear polygon command remove extracted polygon

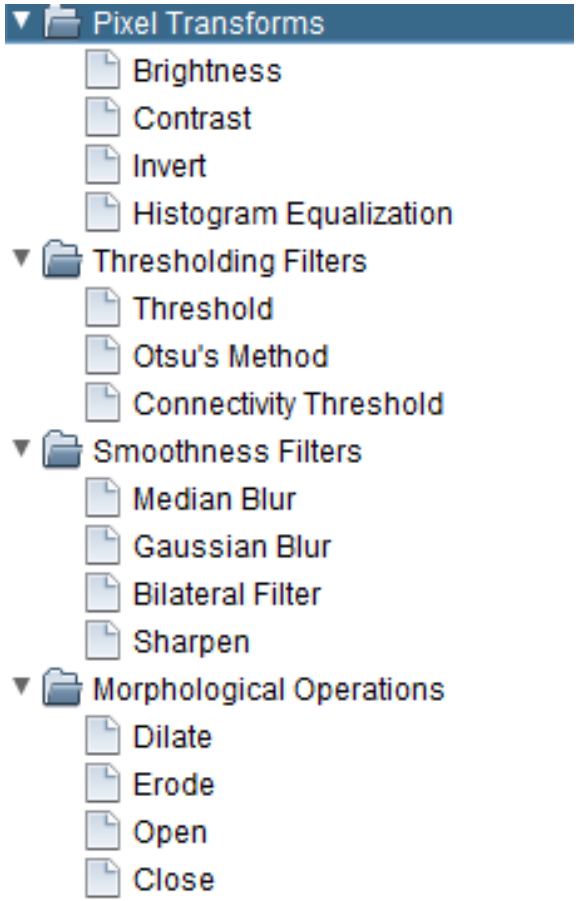


✓ Polygon Tab: Extracts polygon

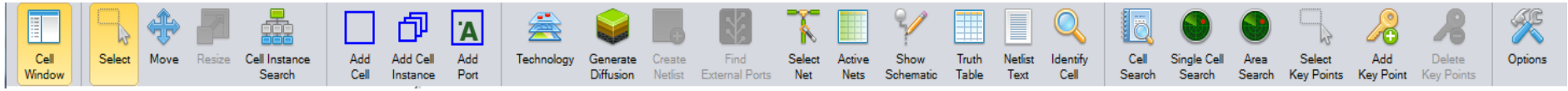
- Manual correction of polygon
- For analysis we will go for digital logic block 1 BUF 270.

Polygon Extraction: Filter

Filter Name	Definition
Histogram equalization	A technique for adjusting image intensities to enhance contrast
Thresholding	Replacing each pixel in an image with a black Pixel if the image intensity is less than some fixed constant or a white pixel if the image intensity is greater than that constant.
Otsu Method	automatically perform clustering-based image thresholding or, the reduction of a gray level image to a binary image
Median Blur	A nonlinear digital filtering technique, often used to remove noise from an image or signal by replacing each pixel by with the median of the neighboring pixels.
Gaussian Method	Same as Median Blur except the function is Gaussian
Bilateral Filter	non-linear, edge-preserving, and noise-reducing smoothing filter for images
Sharpen Filter	A filter for edge enhancement
Dilate	This filter widens and enhances dark areas/bright area of the active layer or selection.
Erode	The opposite operation of dilate
Open filter	Erosion followed by dilation process; removes white spaces

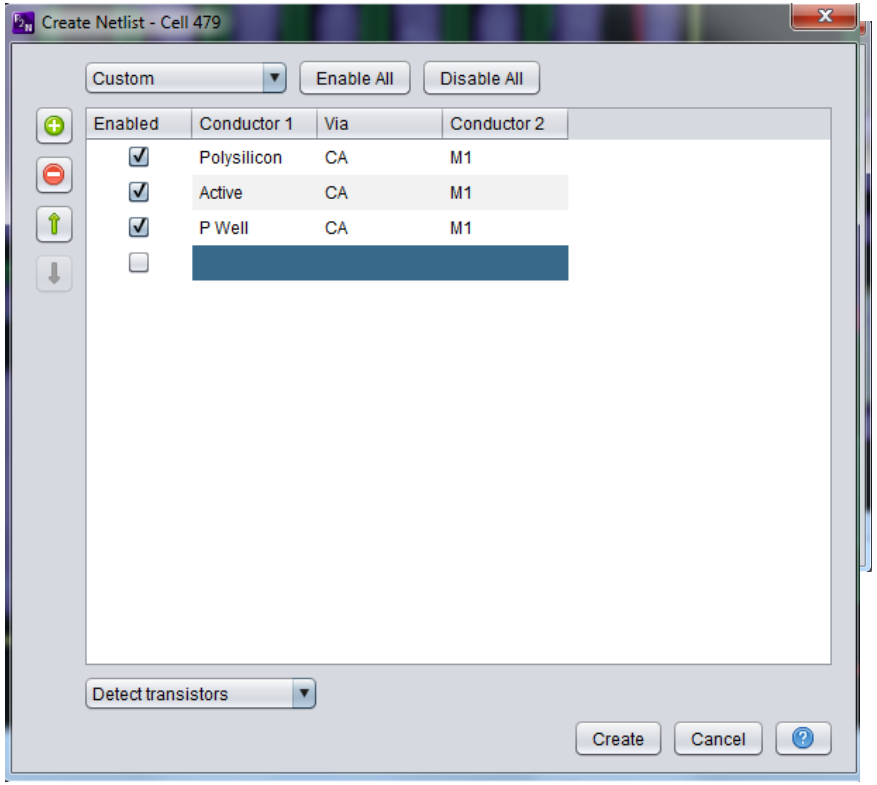


Process Flow



✓ Cell Tab:

- Define cell boundary with add cell command
- Manual pot extraction preferable
- Use select and move to place the port
- Define technology and generate diffusion
- Define connection between layers in create netlist



✓ Netlist Tab:

- Analyze netlist command
- Click show schematic command. The new appear window may show error message. Check the techn ology create netlist command first.

BUF 270.

Question & Answer