

IC Reverse Engineering Netlist Extraction Pix2Net Demo

Mir Tanjidur Rahman

Instructor: Dr. Navid Asadi Zanjani

For Physical Inspection and Attacks on ElectronicS (PHIKS)



- ✓ 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.

10NM ICE LAKE CLIENT Shipping in June

APPROX.

- 2X** Graphics Performance
- 2.5X-3X** AI Performance
- 2X** Video Encode
- 3X** Wireless Speeds

Disclaimer: Results are approximate and have been estimated or simulated as of April 2019 using Intel internal analysis or architecture simulation or modeling
Graphics and video – Next Gen Graphics Iris Plus Experience
Wireless – Intel's Wi-Fi 6 (GIG+) vs typical competitive 11AC design
AI – AIXPRT Community 2 Preview; OpenVINO 2018.R5, Max Throughput 15W WHL to 15W ICL projection

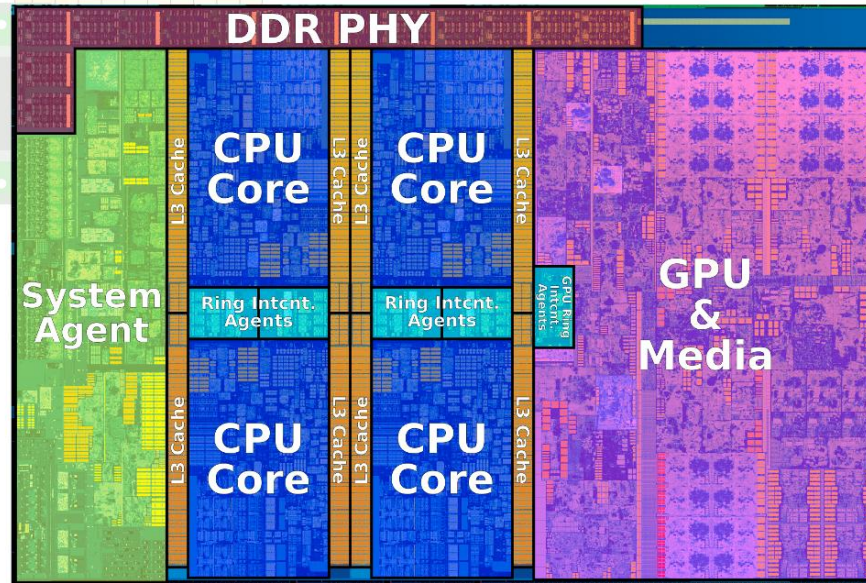
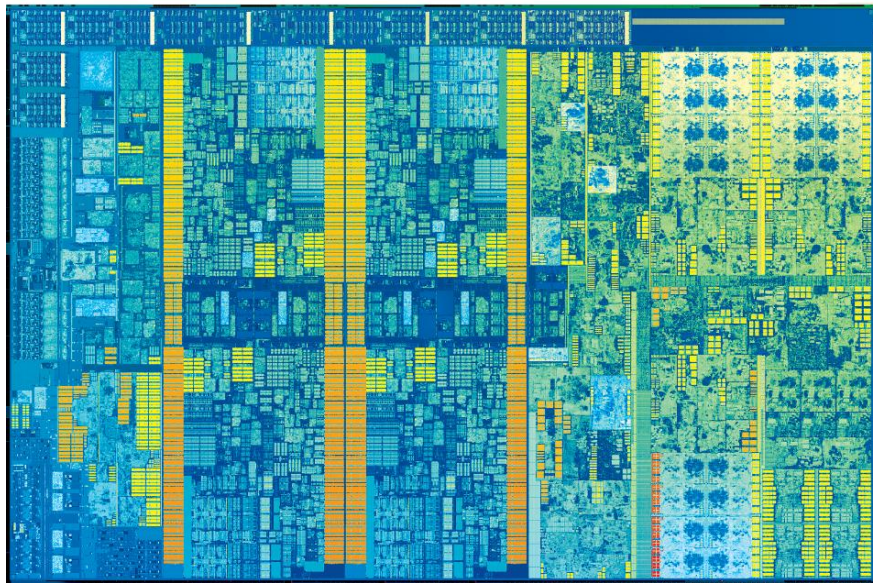
For more complete information about performance and benchmark results, visit www.intel.com/benchmarks. Performance results are based on testing as of date specified and may not reflect all publicly available security updates. See configuration disclosure for details. No product or component can be absolutely secure.

intel 2019 INVESTOR MEETING

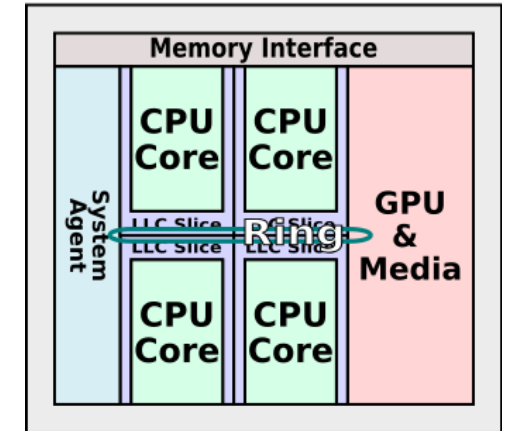
15

Wiki

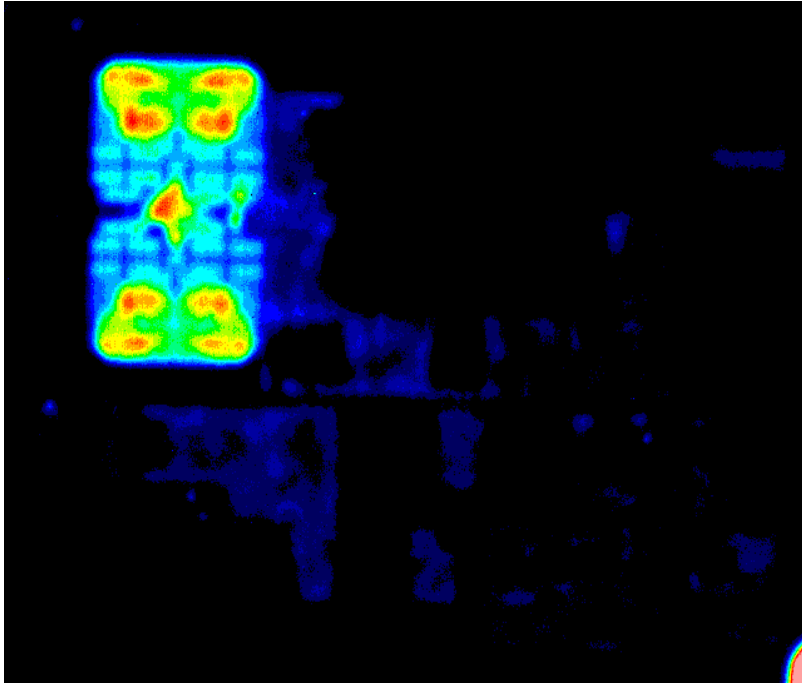
Core i7-7700K



Kaby Lake



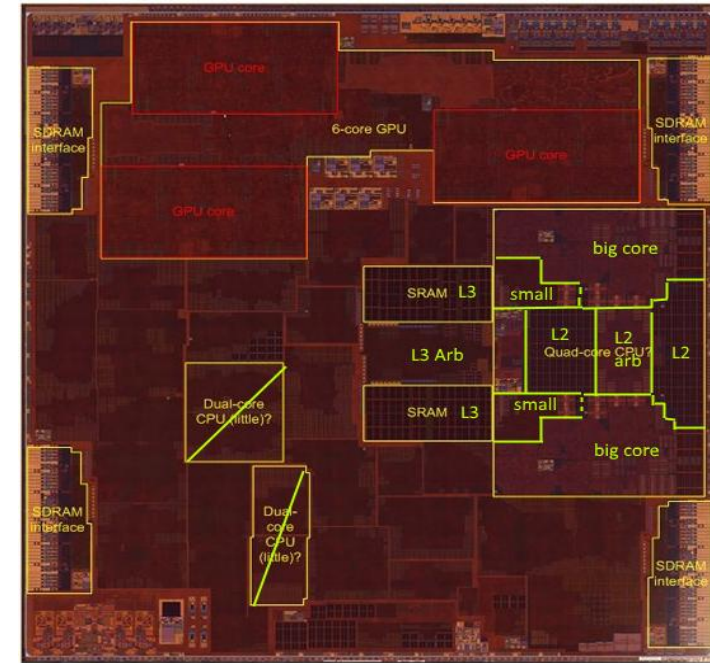
- Memory location, BUS, cache, etc. can be distinguished from repetitive pattern in the device
- Logic areas are highly irregular areas and easily differentiable from memory or cache.



Work Completed by Dhvani Mehta for PAINE Wrokshop

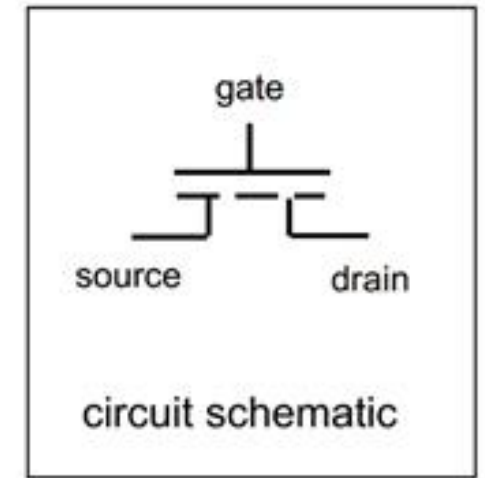
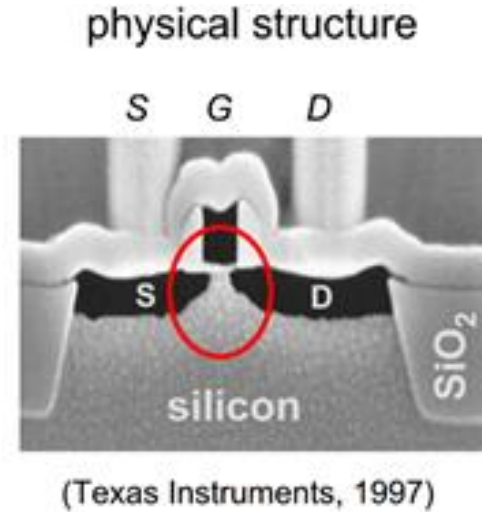
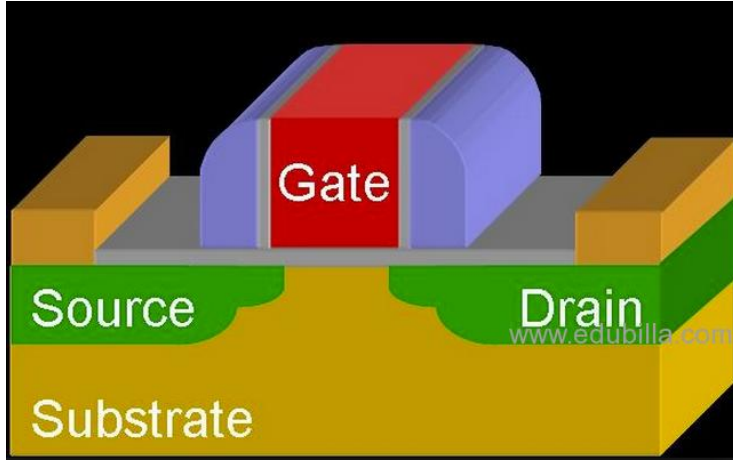
- CORE, cache, registers can also be identified from photonic emission analysis; but that's a different story we will learn later in the course

Hardware IPs implemented In Apple A10 Quadcore SoC

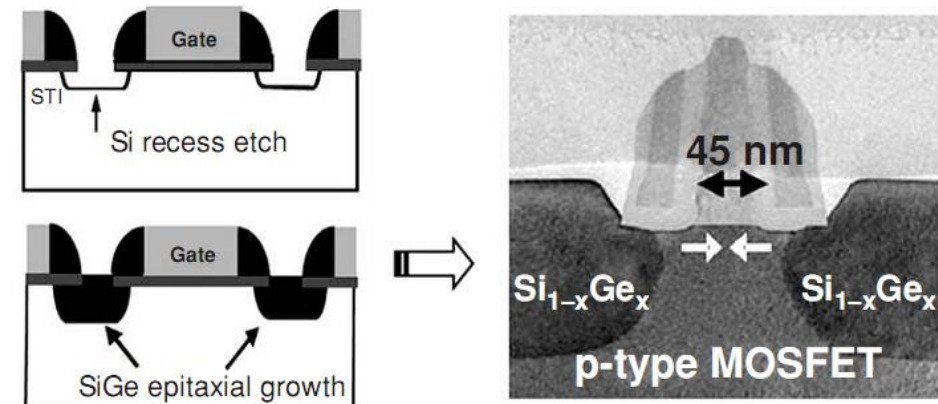
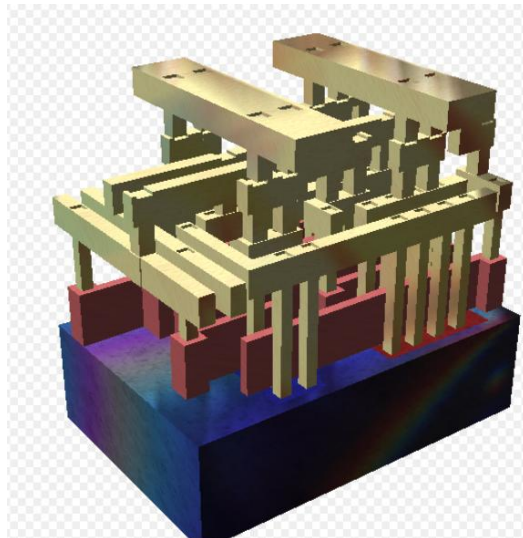


- TSMC's **16 nm** FinFET
- **3.3 billion** transistors
- Die size: 125 mm²

VLSI & Fabrication Process: Planer MOSFET

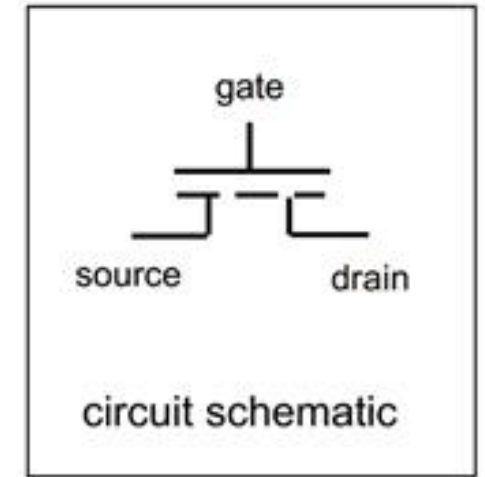
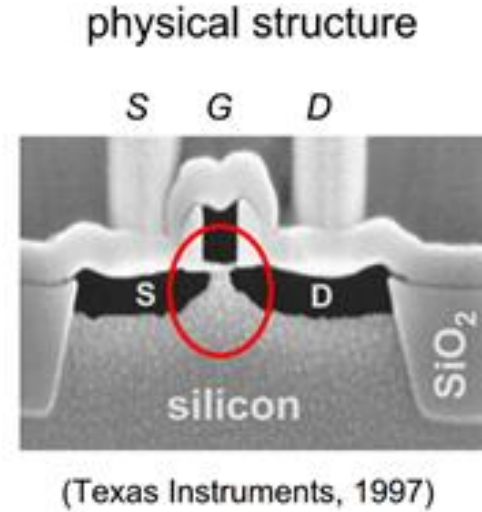
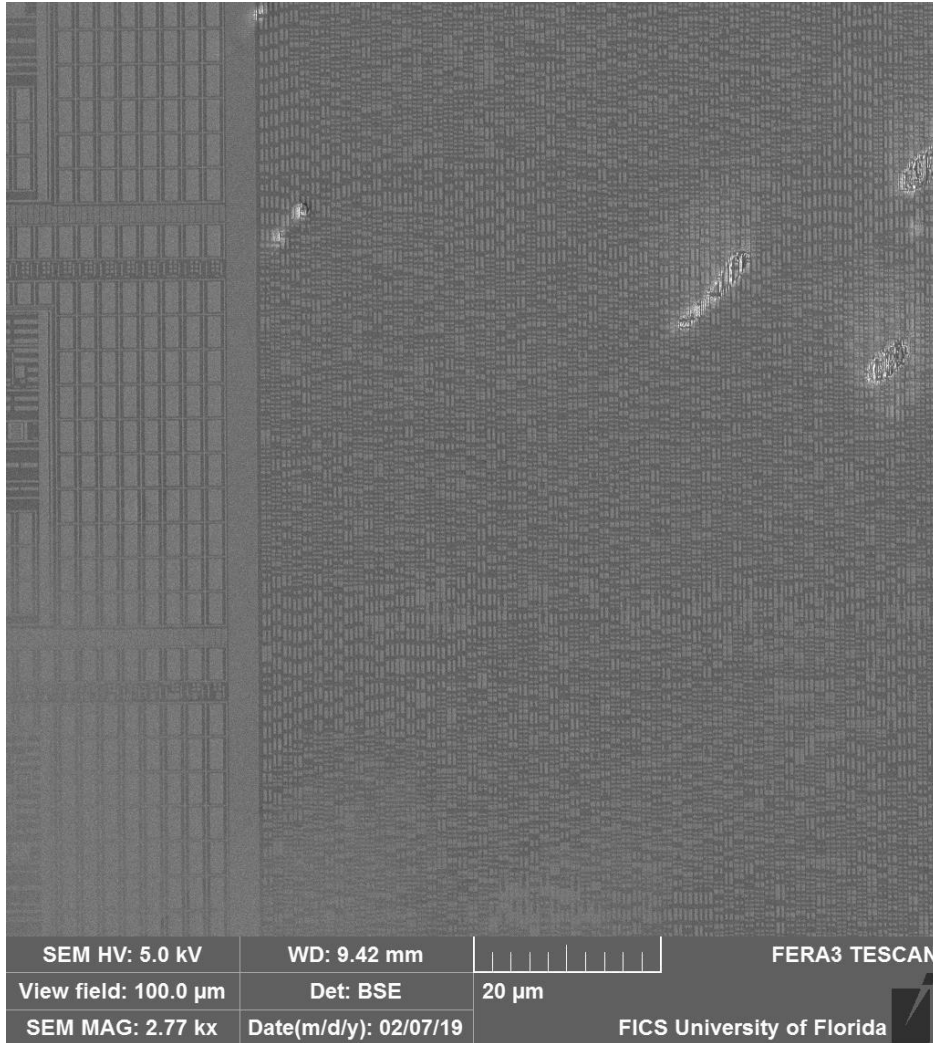


Planner MOSFET

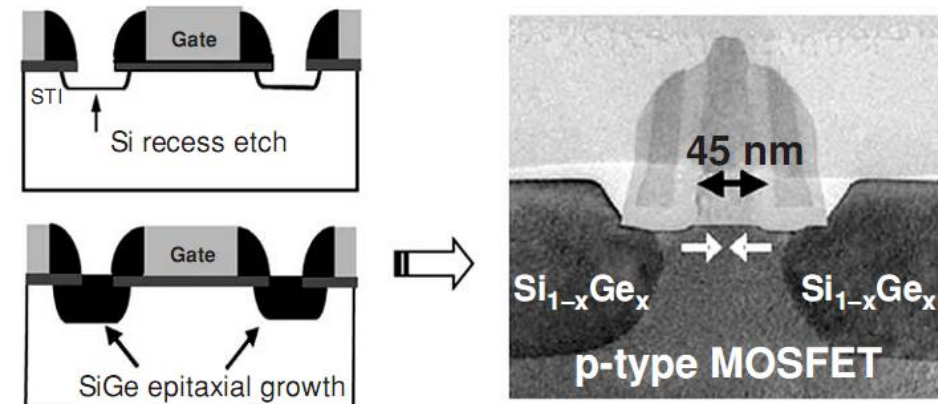


Equal width p and n-type MOSFET

VLSI & Fabrication Process: Planer MOSFET

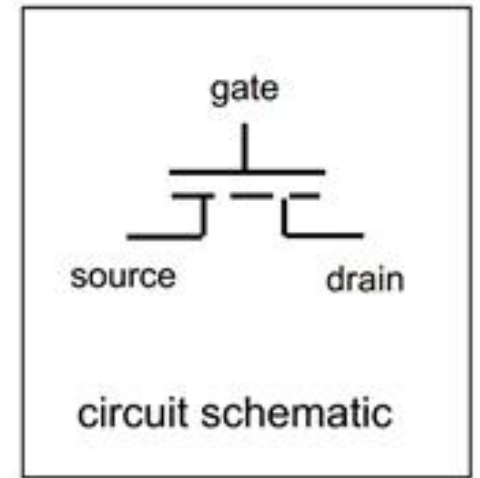
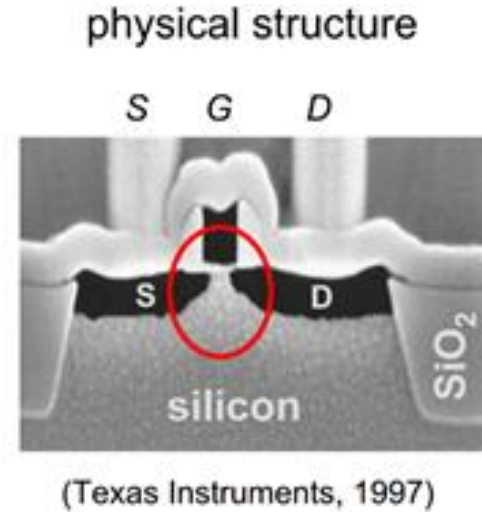
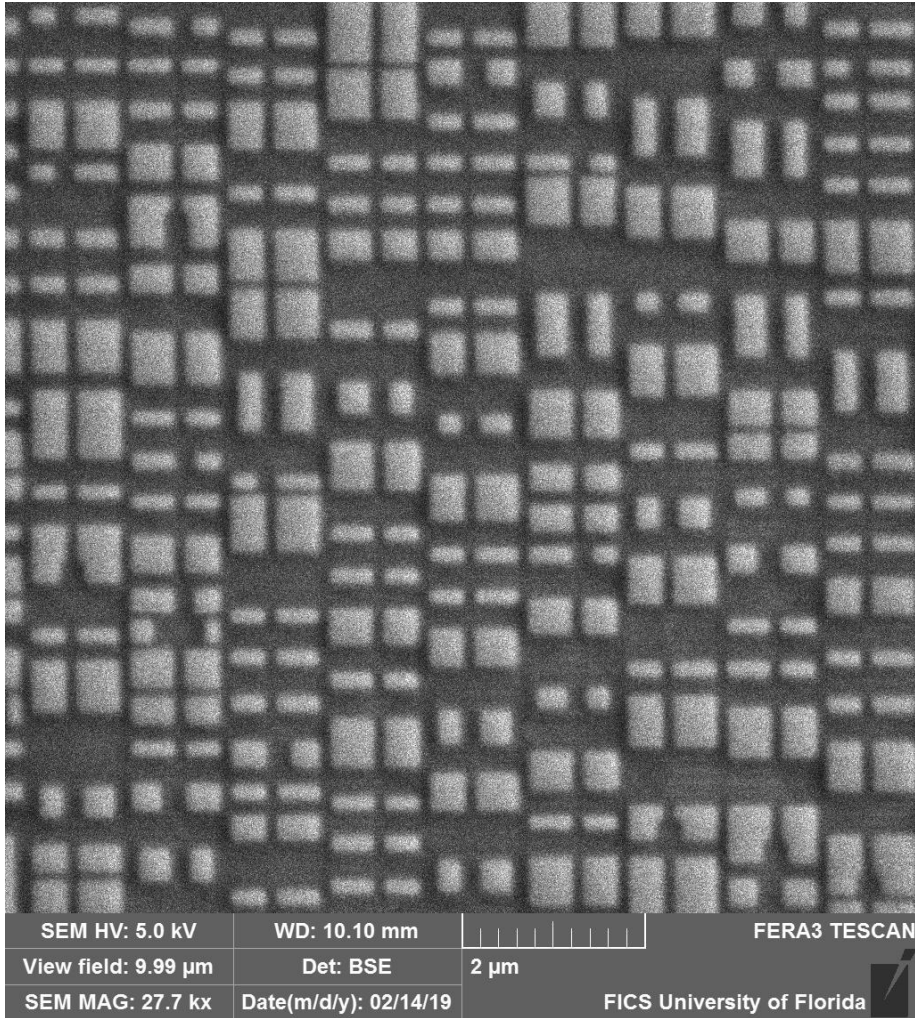


Planner MOSFET

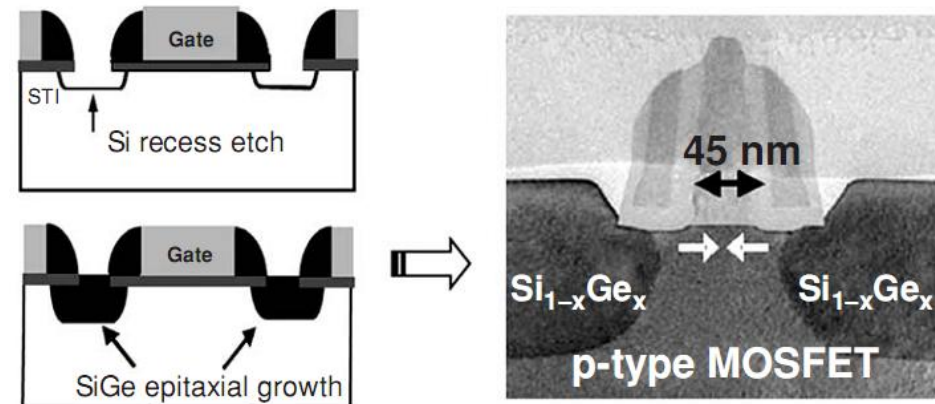


Equal width p and n-type MOSFET

VLSI & Fabrication Process: Planer MOSFET

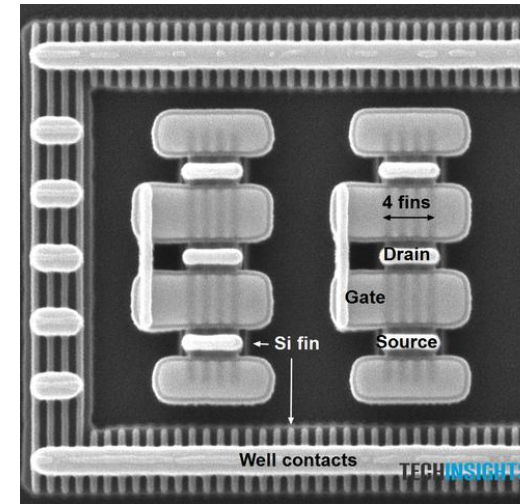
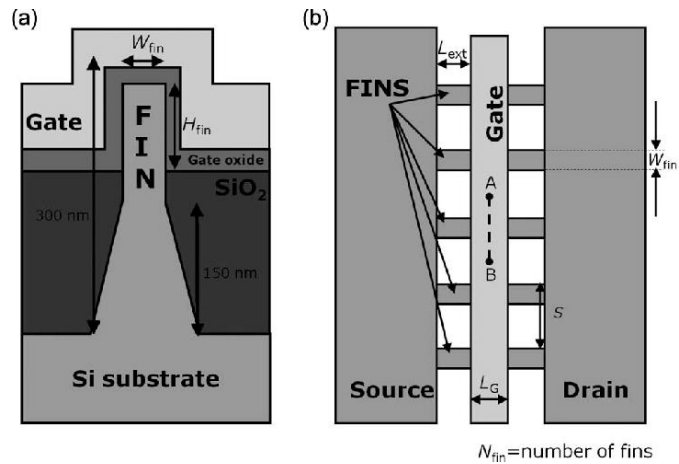


Planner MOSFET



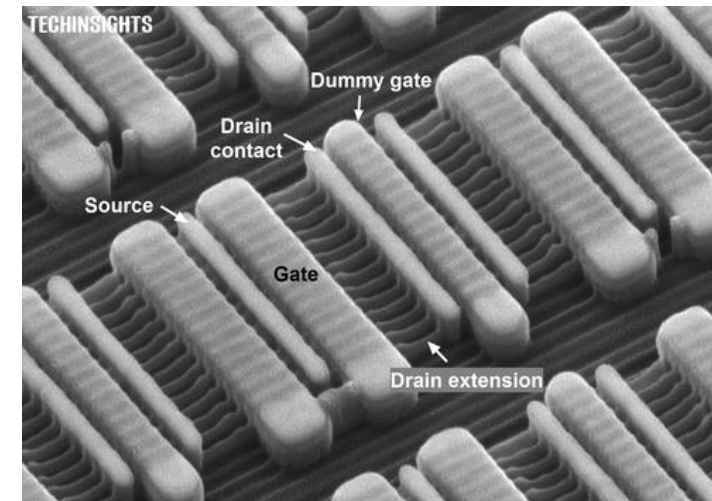
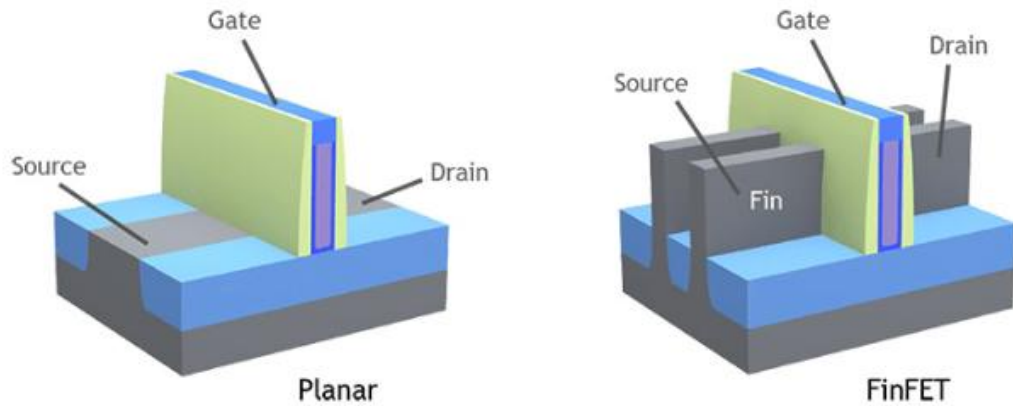
Equal width p and n-type MOSFET

VLSI & Fabrication Process: FinFET MOSFET



Cross section and top view of FINFET

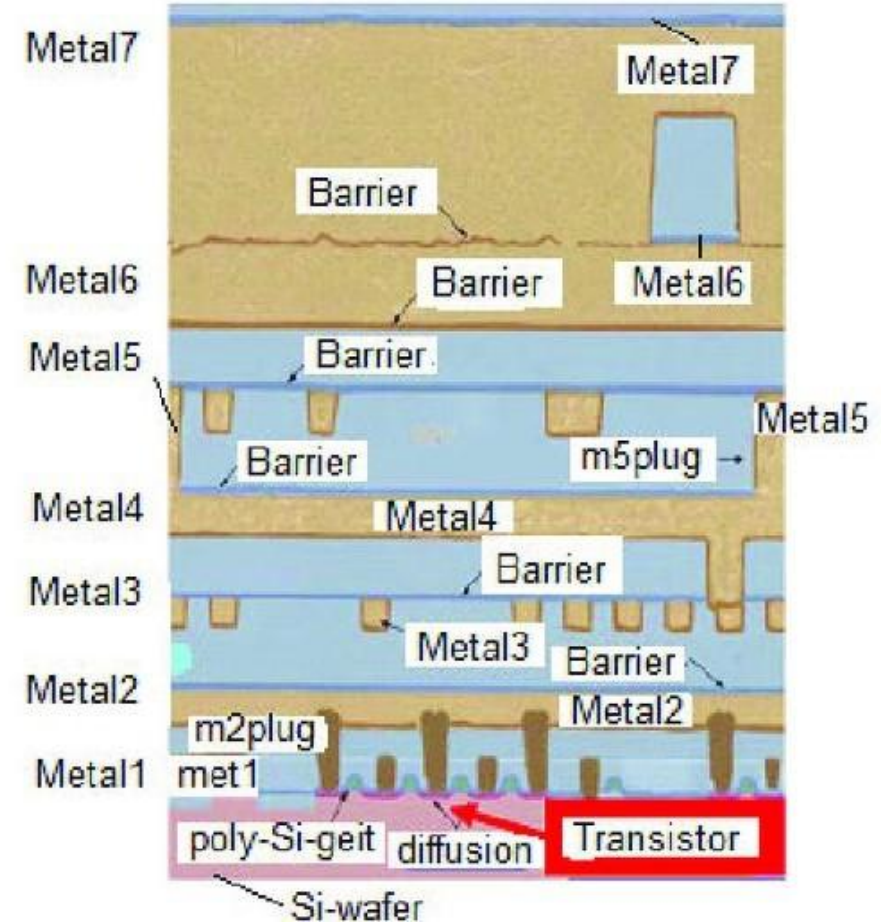
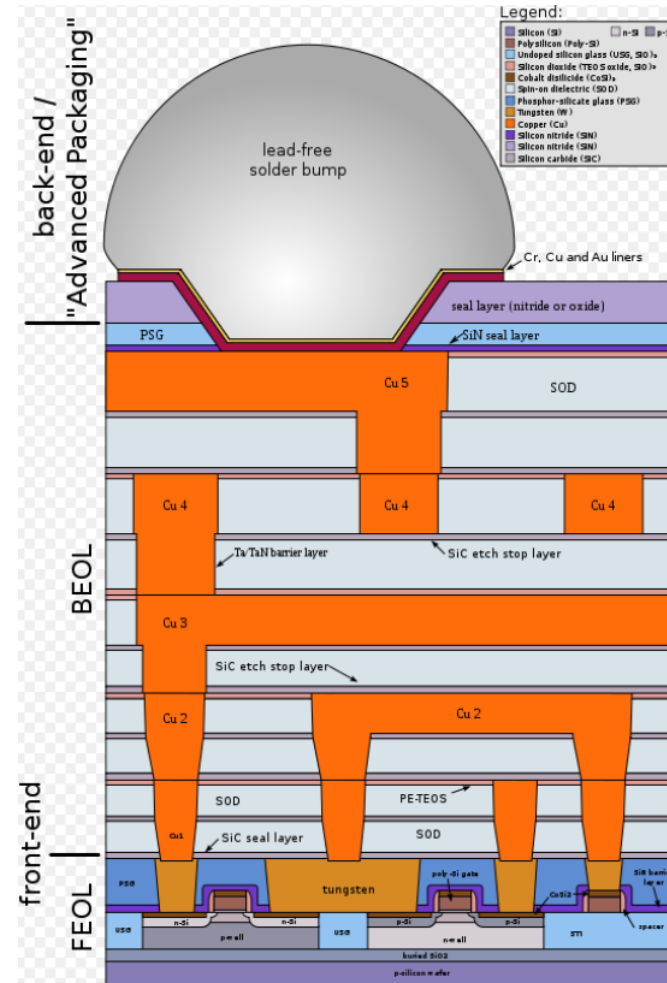
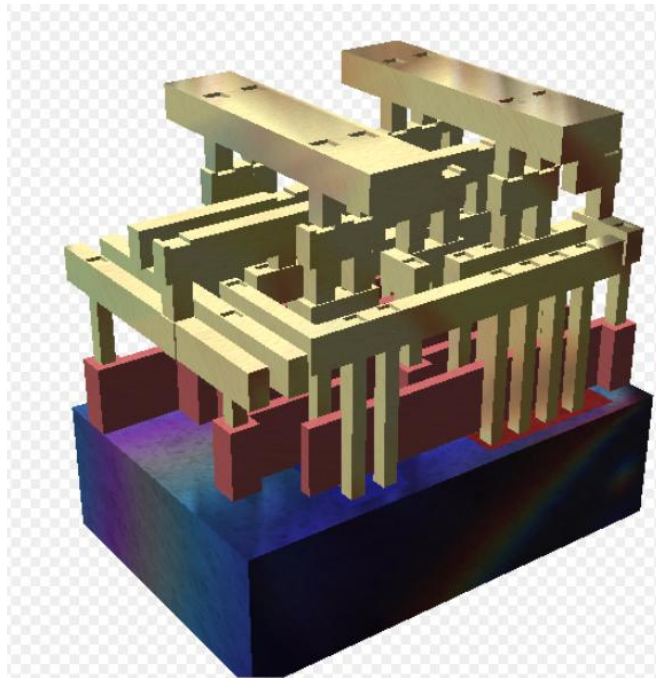
Source: Time-dependent dielectric breakdown on subnanometer EOT nMOS Finfet



Planner MOSFET Vs FINFET

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

VLSI & Fabrication Process: Metal Layers and Vias

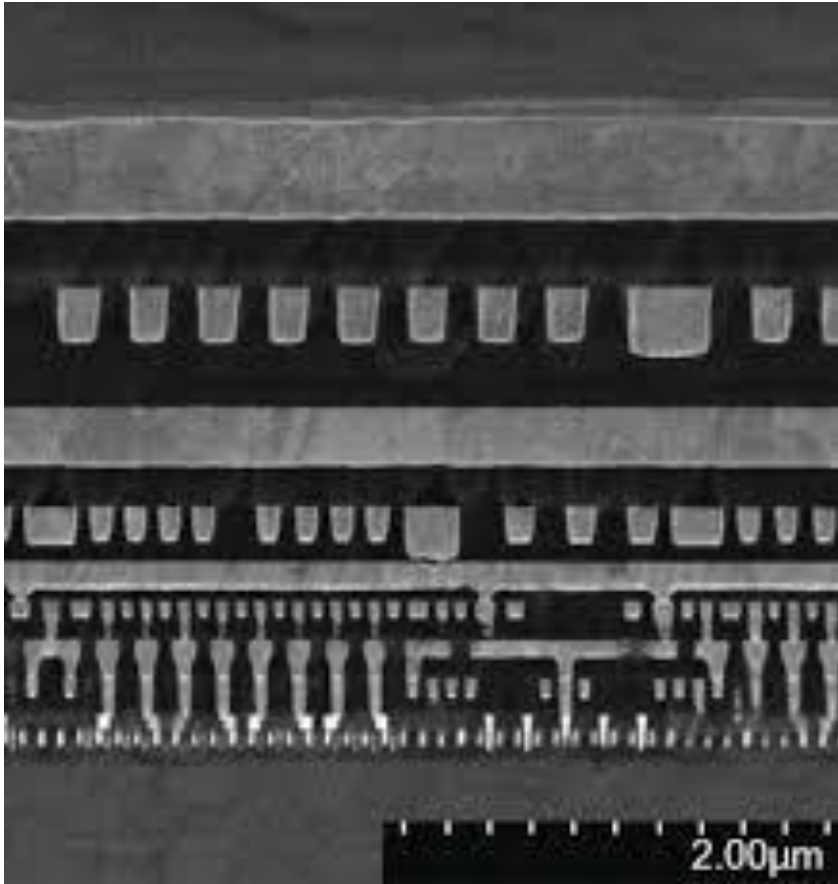


- Model cross section of ICs

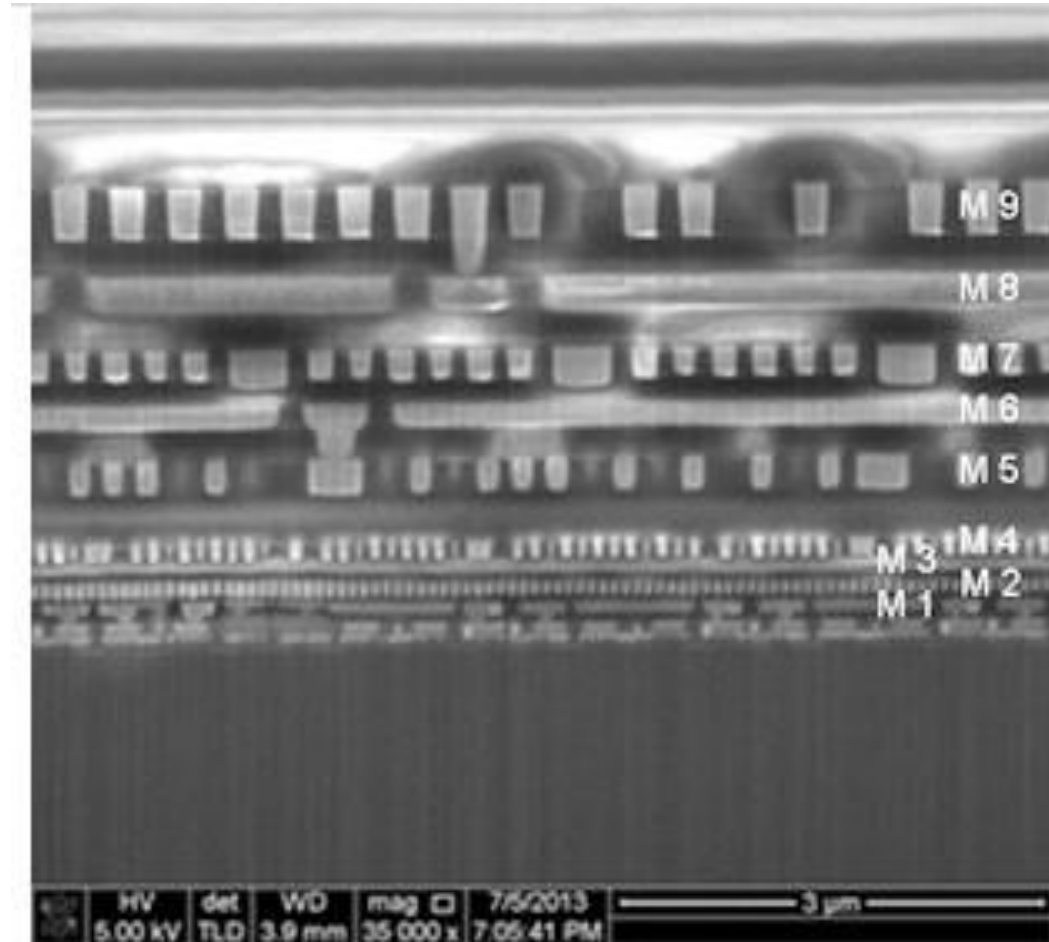
Watch List: 1. <https://www.youtube.com/watch?v=d9SWNLZvA8g>
 2. <https://www.youtube.com/watch?v=uVWHxggc-O94>

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

VLSI & Fabrication Process: Metal Layers and Vias



SEM image of different metal layers and transistors



Different metal layers in the SEM image cross section

Reverse Engineering Workflow and the Outcome

Reverse Engineering Steps

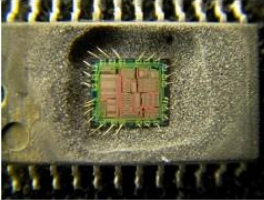


Imaging
- SEM/ Optical

Depackaging
- Frontside
- Backside



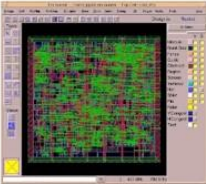
Clean & Prep
(Planarize)



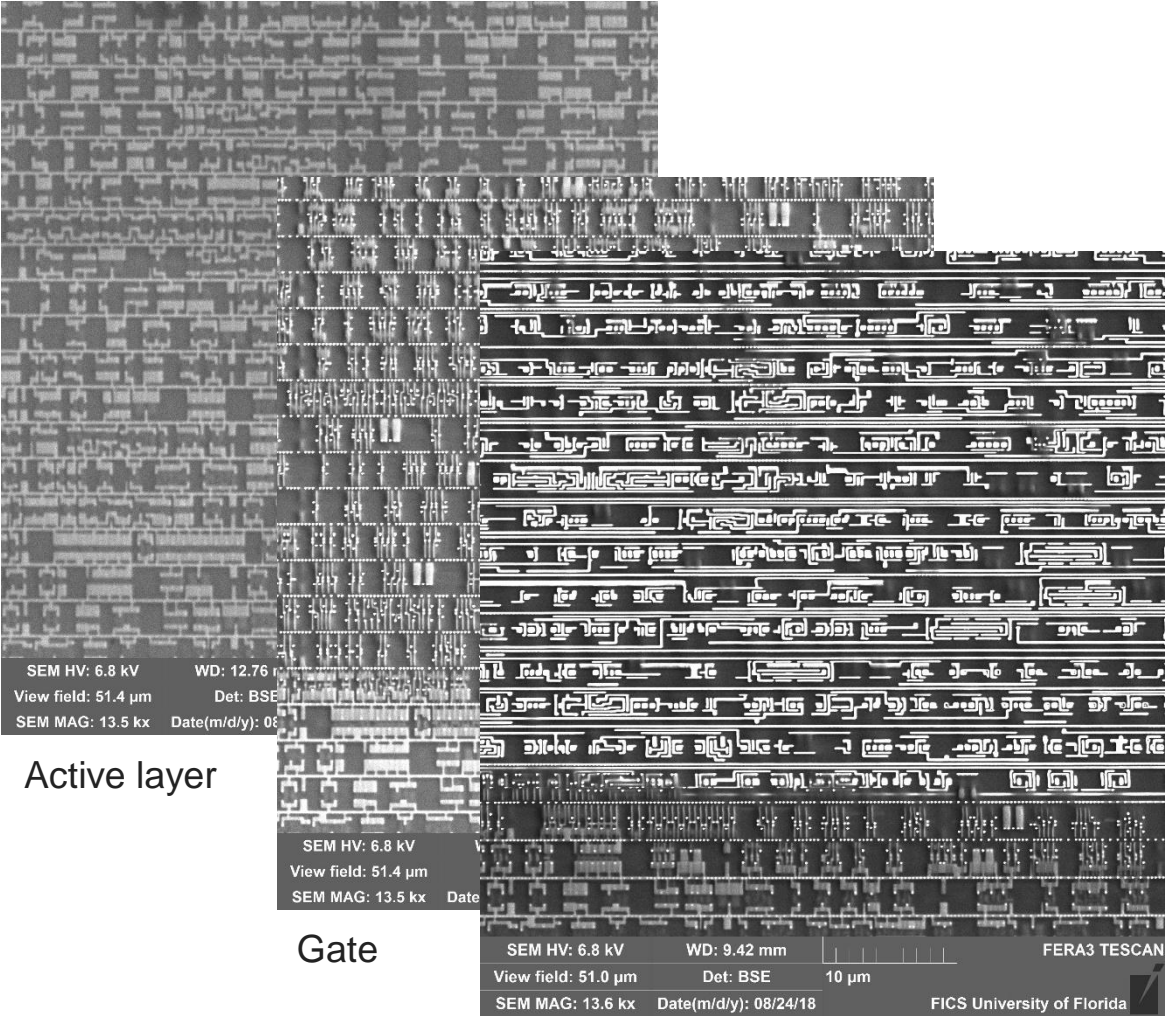
Delayering
- Plasma/FIB etching
- Wet etching



Extract Netlist
- Pix2Net
- Chipjuice



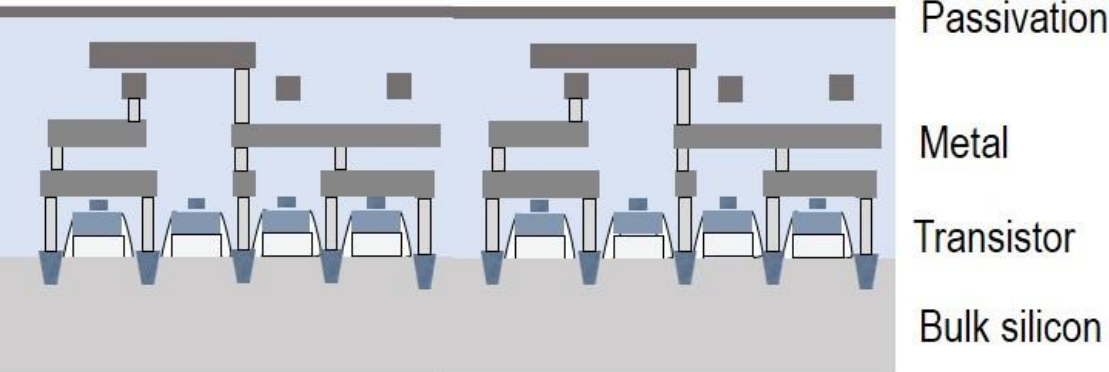
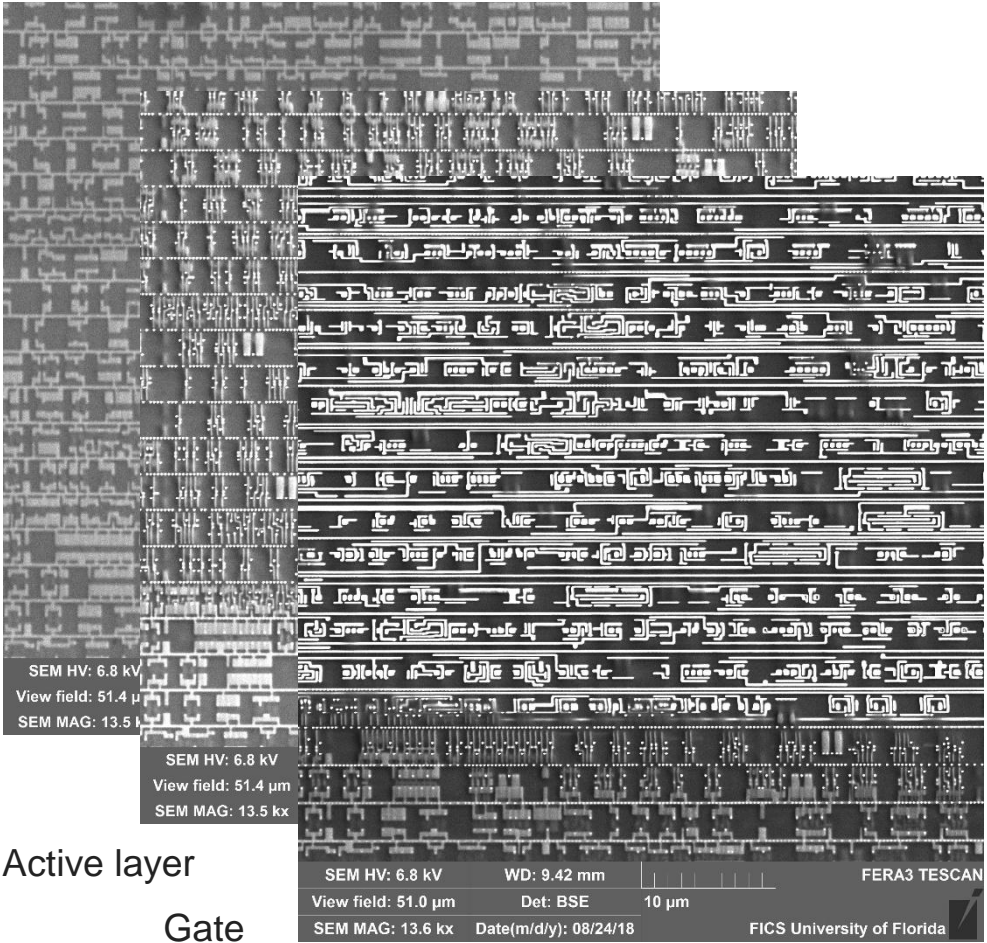
Outcome of Process



Metal layers

Understanding the Connection in SoCs

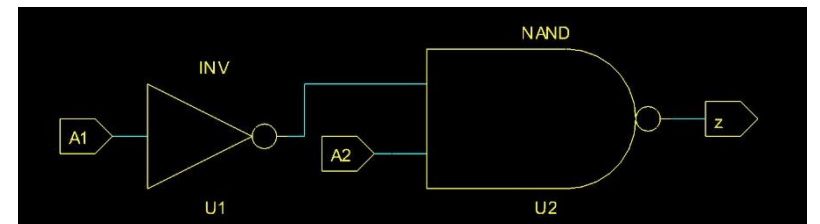
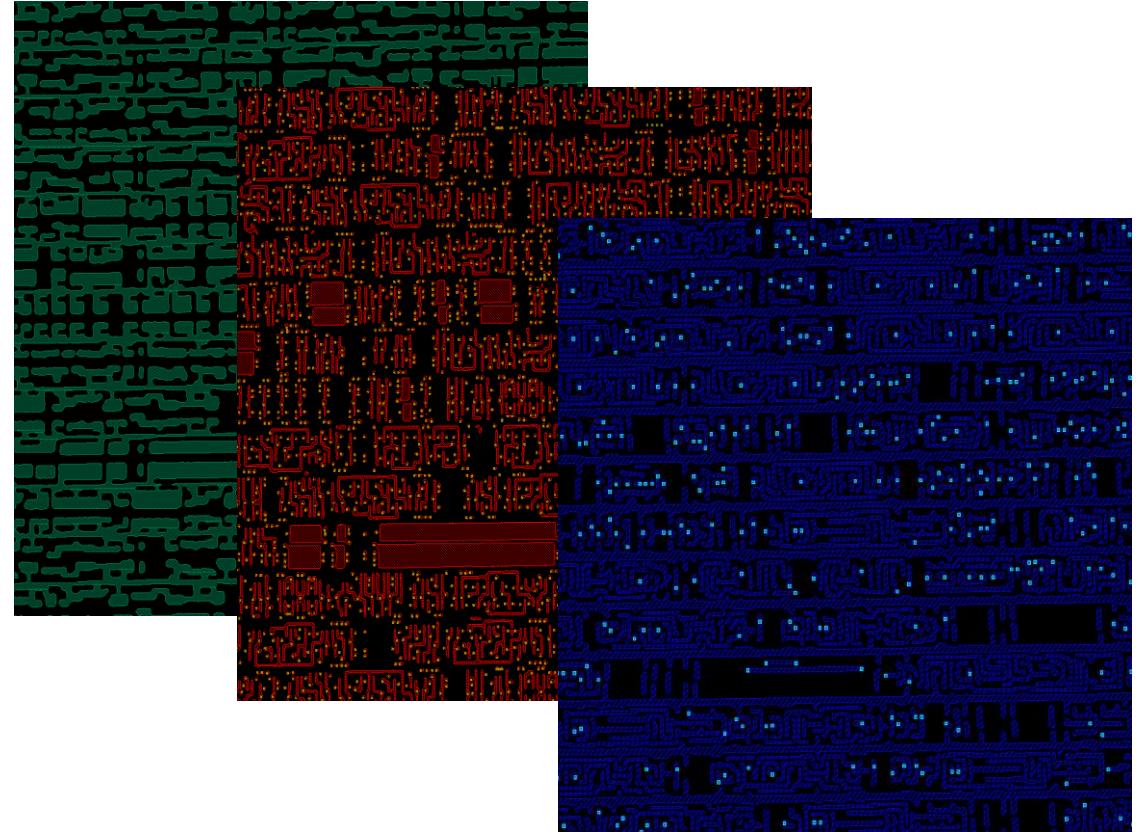
Outcome of Process



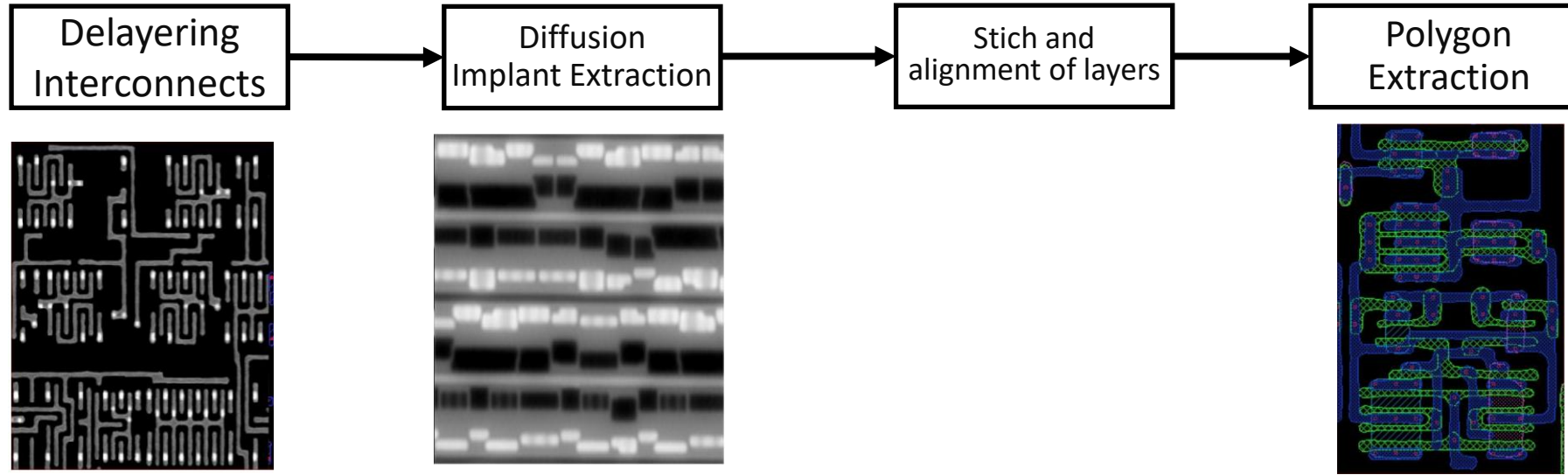
After overlaying, the layers should be aligned at the same way, they were aligned in the device. Otherwise the connection diagram will be wrong.

Challenges of 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

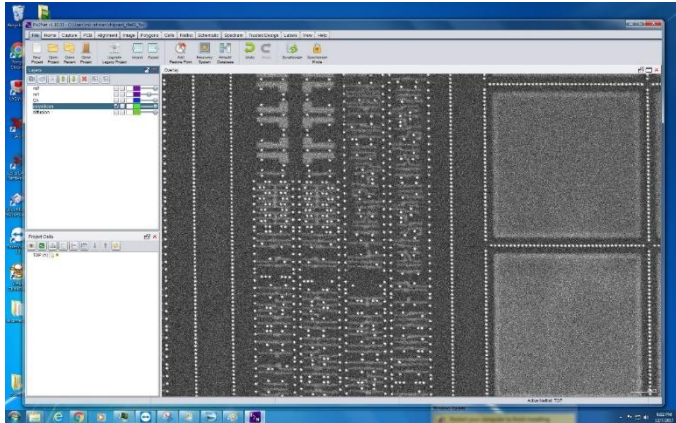


Workflow of Netlist Reverse Engineering

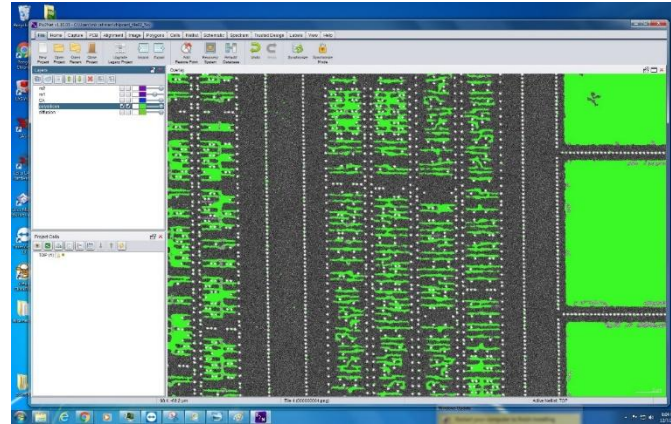


Polygon Extraction

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

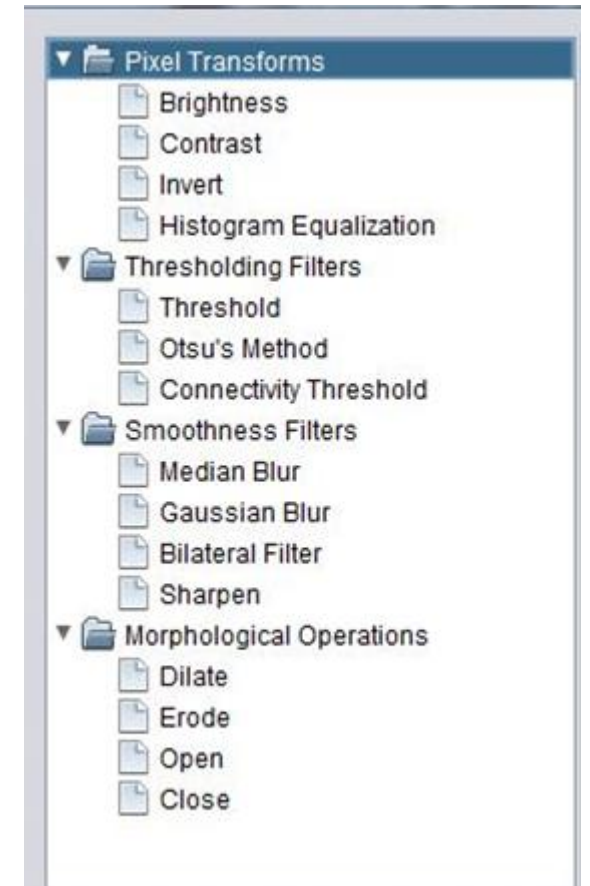


SEM image

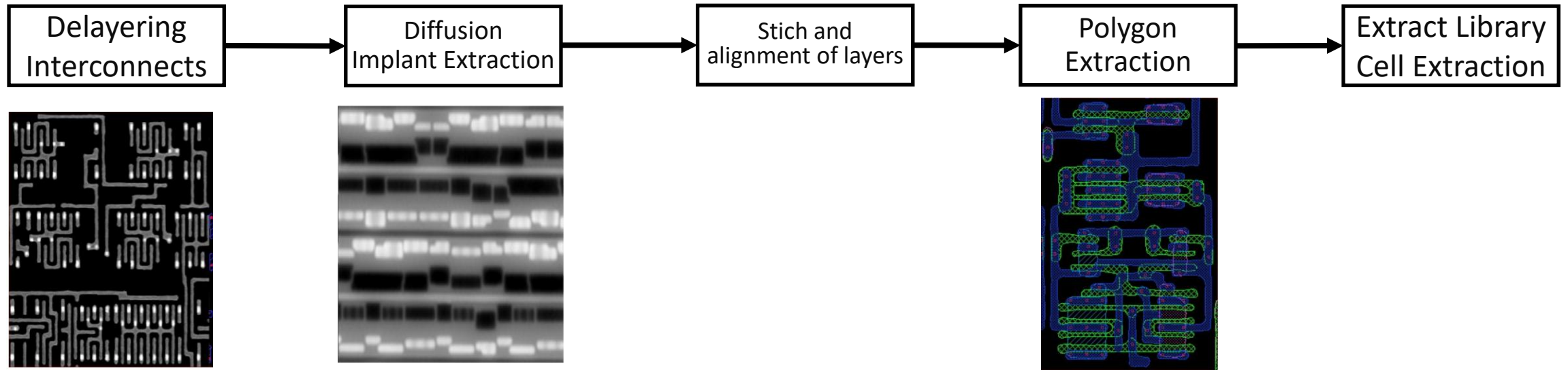


Polygon Extracted image

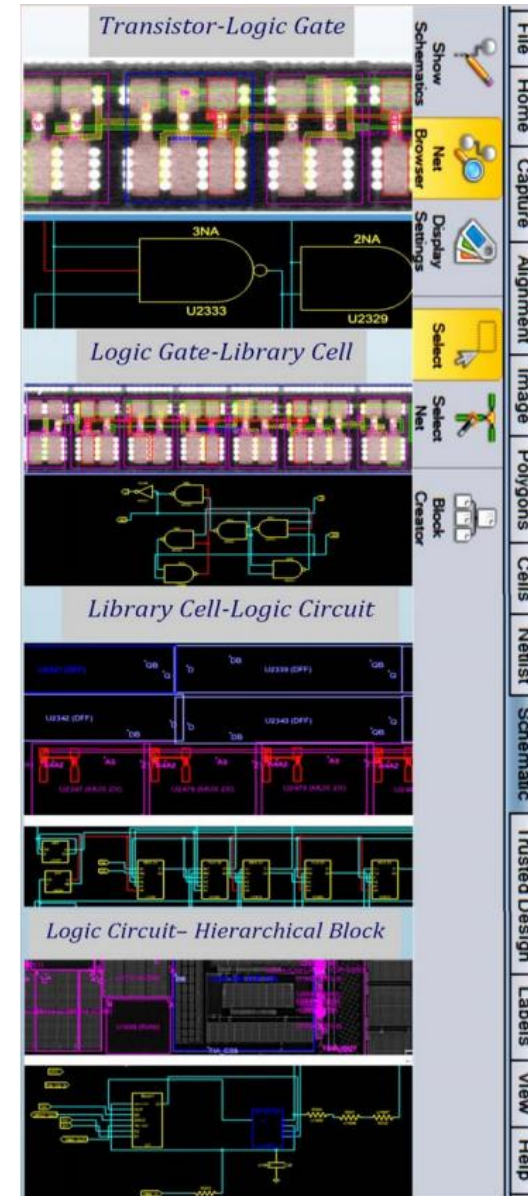
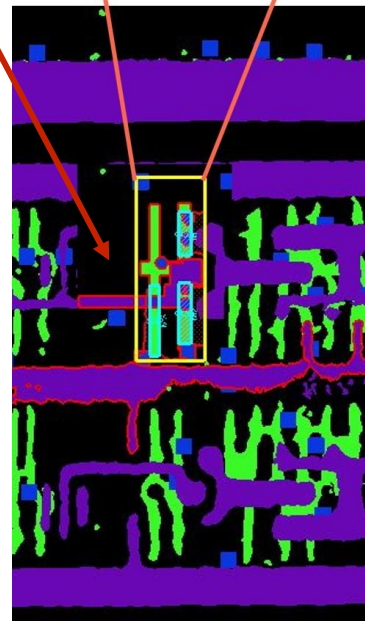
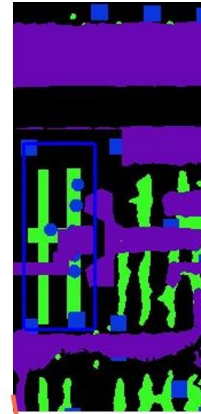
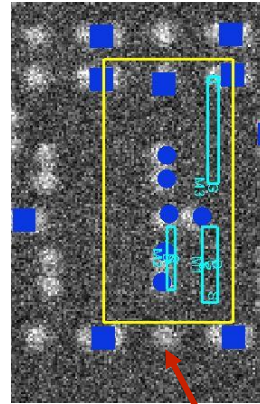
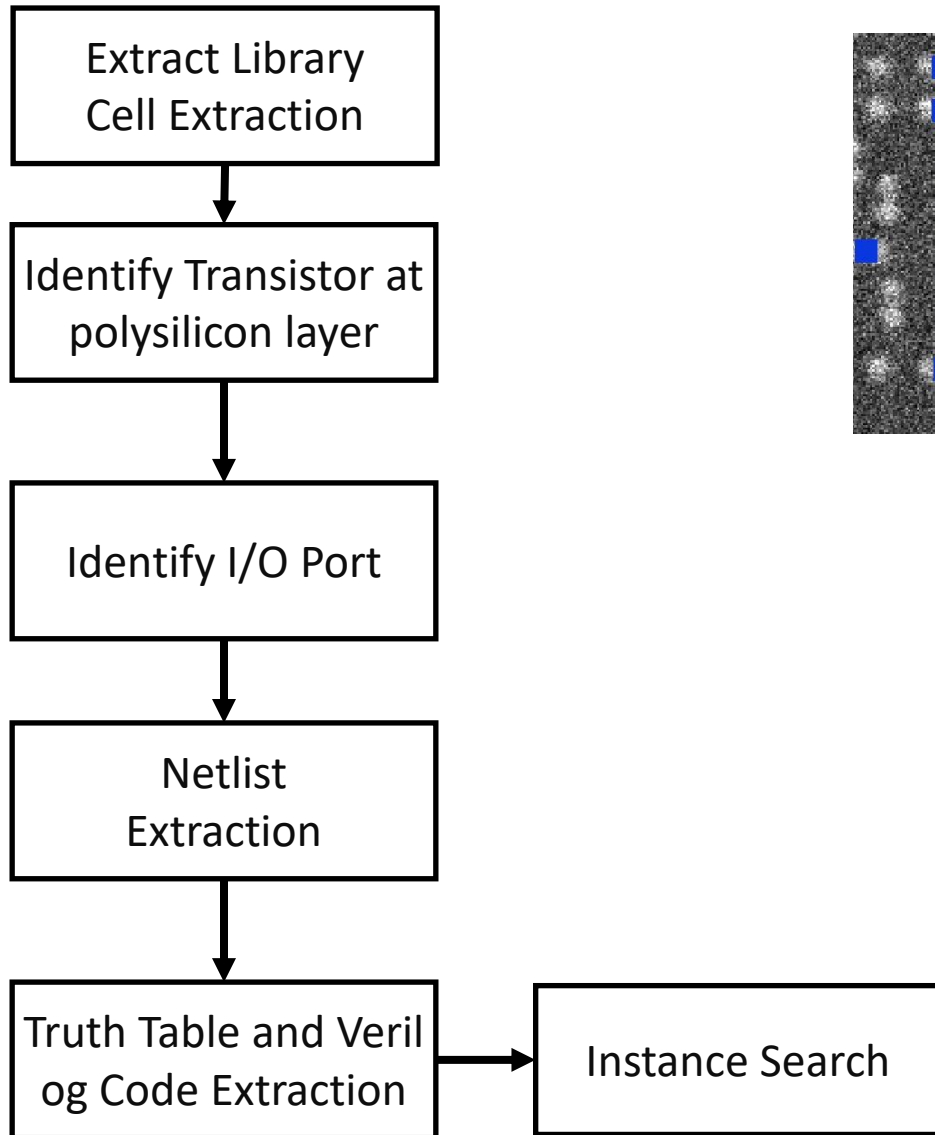
- Accuracy of polygon extraction significantly effect the accuracy and effort required for circuit extraction
- Several in-built filters are available in Pix2Net software to improve the image quality



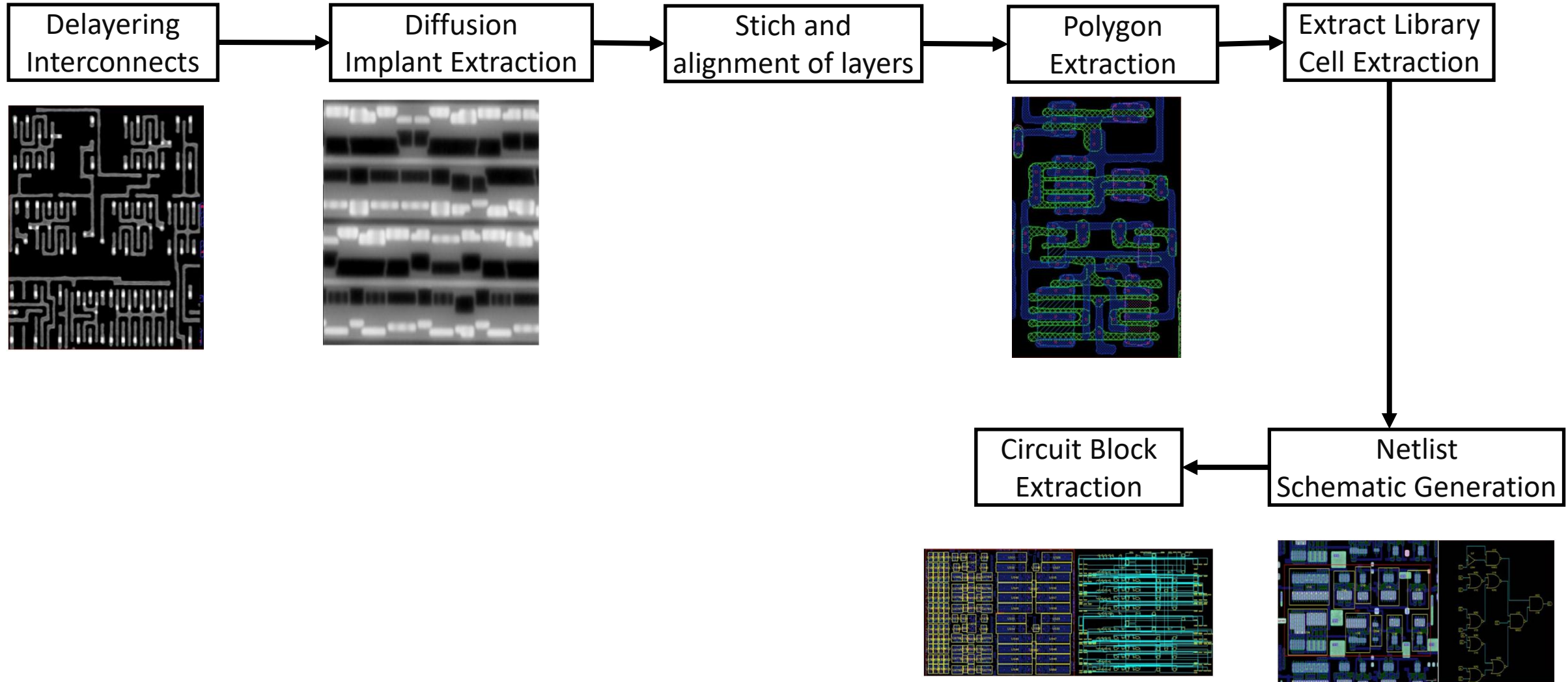
Workflow of Netlist Reverse Engineering



Workflow of Netlist Reverse Engineering



Workflow of Netlist Reverse Engineering



Logic Gate Structure

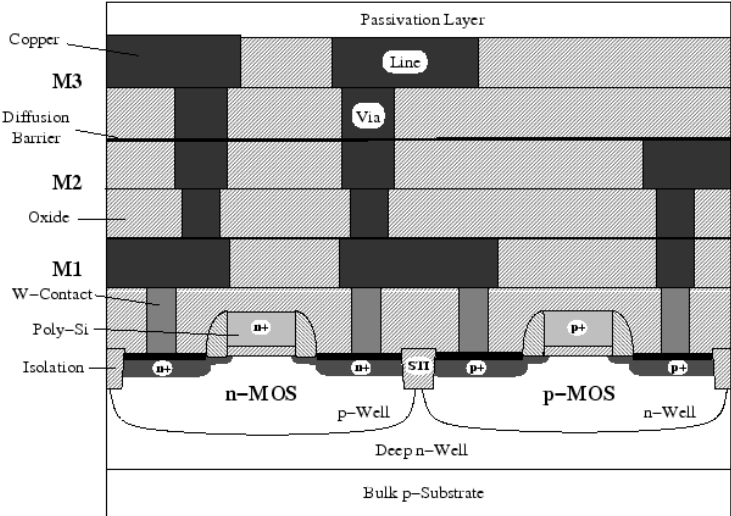
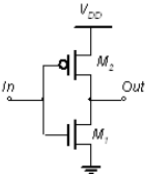
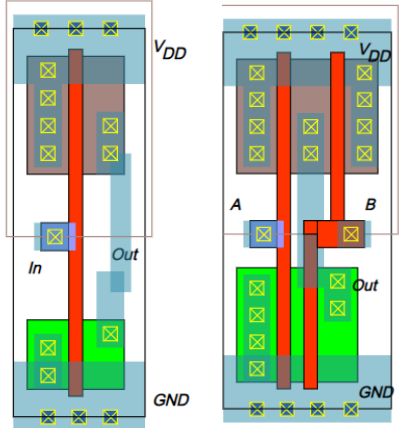


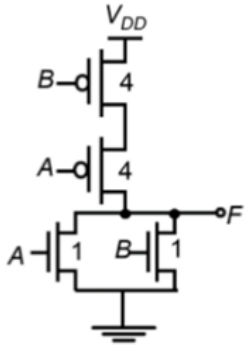
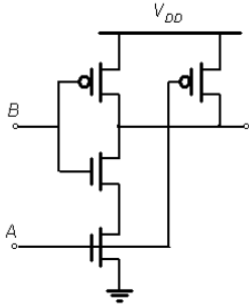
Figure 1.1: Schematic cross-section of a final CMOS integrated circuit with an interconnect structure of three metal layers (M1 - M3).



Inverter circuit



2-input NAND gate



N M O S				
	Drain	Drain	Drain	Drain
	Source	Source	Source	Source
	Gate	Gate	Gate	Gate
P M O S				
	Drain	Drain	Drain	Drain
	Source	Source	Source	Source
	Gate	Gate	Gate	Gate

NMOS and PMOS transistor Symbols

Image Quality and Trojan Scanner

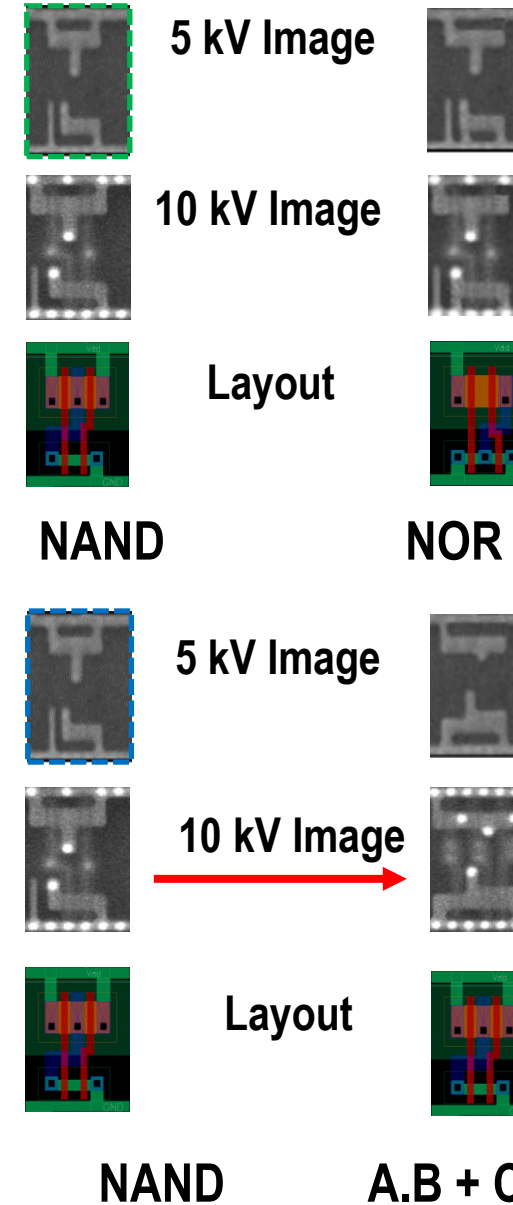
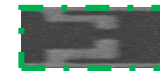
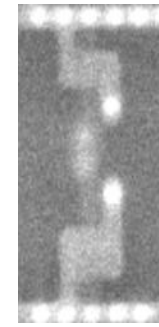


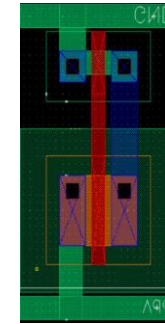
Image Quality and Trojan Scanner



5 kV Image



10 kV Image

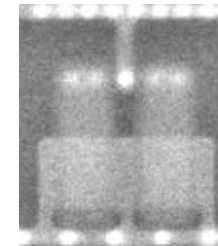


Layout

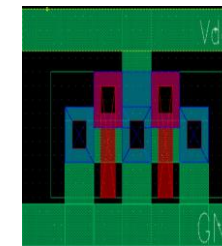
Inverter



5 kV Image



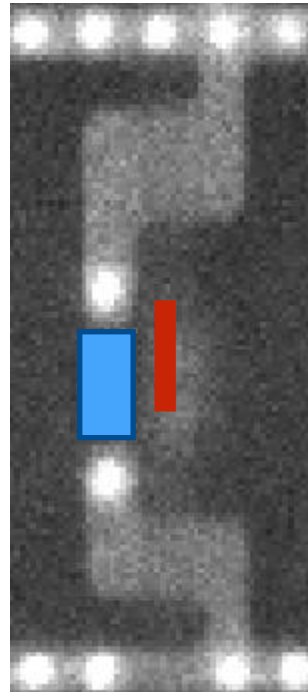
10 kV Image



Layout

MOS Capacitor

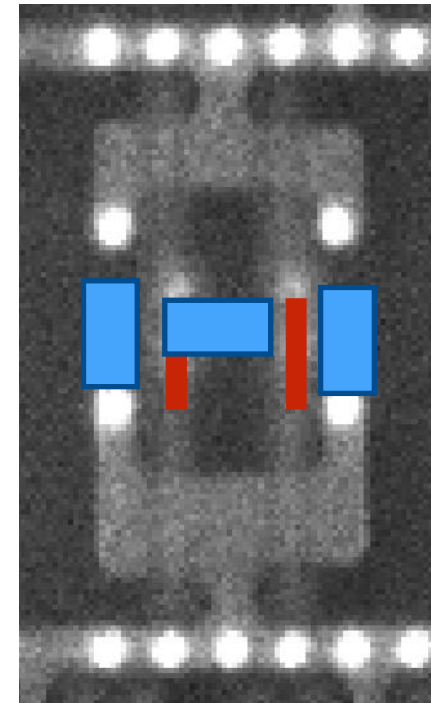
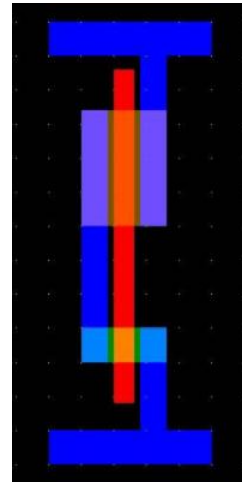
Manual RE: Logic Extraction



PMOS

NMOS

Inverter

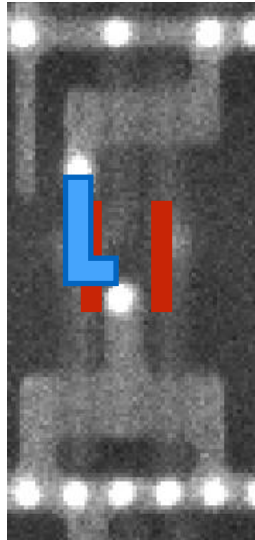


NMOS

PMOS

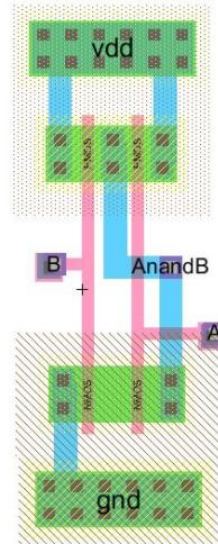
Buffer

Practice Problem



NMOS

PMOS



NAND

Pix2Net Layout

The screenshot shows the Pix2Net software interface with several key components highlighted by red boxes and labels:

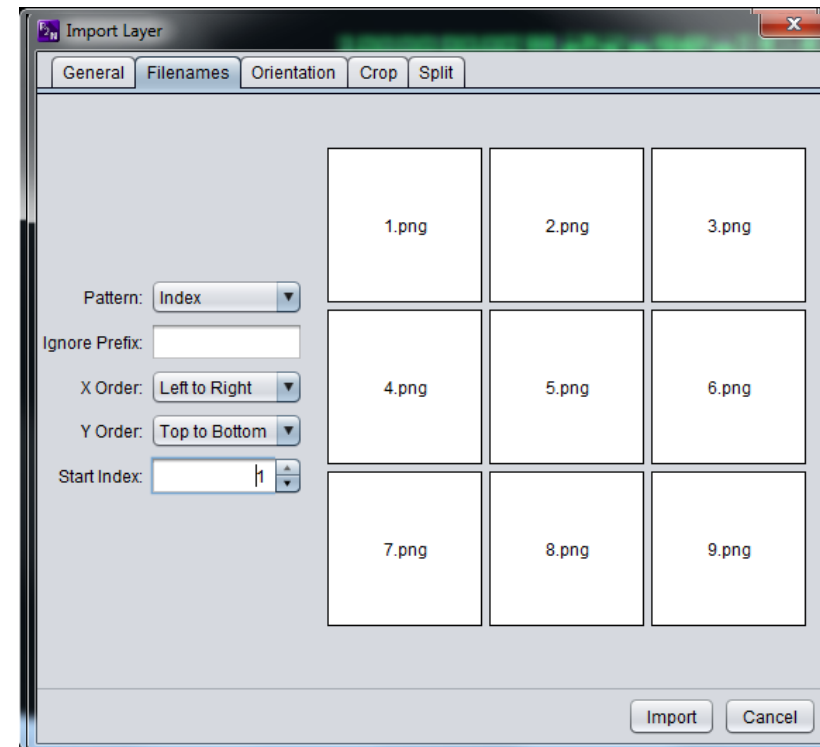
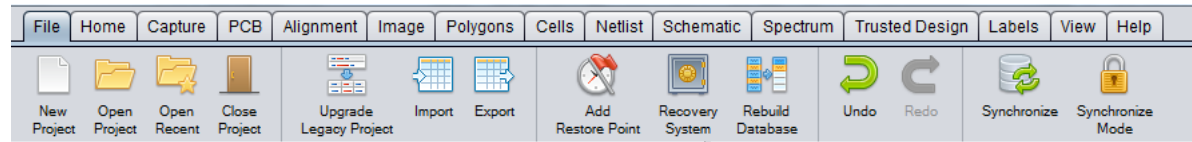
- Task Navigator:** Located at the top right, it contains a menu bar (File, Home, Capture, PCB, Alignment, Image, Polygons, Cells, Netlist, Schematic, Spectrum, Trusted Design, Labels, View, Help) and a toolbar with icons for Show Schematic, Net Browser, Display Settings, Select, Select Net, Block Manager, Block Nets, and Logic Block Search.
- Image/GDS II Layer:** A panel on the left side of the interface, listing various layers such as M8, Via 7, M7, Via 6, M6, Via 5, M5, Via 4, M4, Via 3, M3, Via 2, M2, Via 1, M1, CA, Polysilicon, Active, P Well, Location_OV, Generated Diffusion, and Generated Transistors.
- Image/polygon view:** The central workspace displaying a detailed layout of a circuit board with a grid and various components.
- Library /extracted cell:** A panel on the left side, showing a hierarchical tree structure of components under 'TOP (1)', including Dig Block 1 (53), BLOCK 0 ARRAY (478), and LOGIC BLOCK 1 (473).
- Task Manager Bar:** A panel at the bottom right, displaying a table of tasks and their progress.
- Compiler Message:** A panel at the bottom right, displaying compiler messages, with a red arrow pointing to a message icon.

Task	Progress	State	Elapsed	Remaining
Netlist	Tracing Modified Polygons: 0 / 0	Finished	00:00:00	00:00:00
Via 1: Extracting polygons		Finished	00:00:21	00:00:00
Netlist		Finished	00:00:01	00:00:00

✓ 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

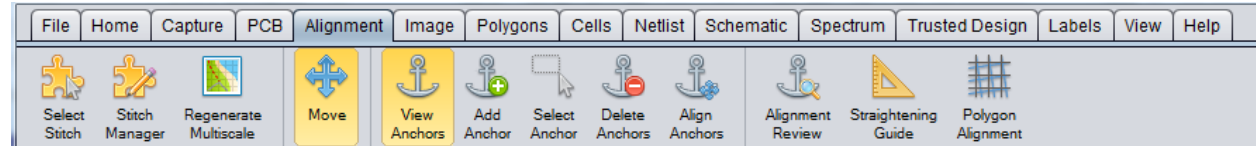
Note: For any detail information check help tab



Process Flow

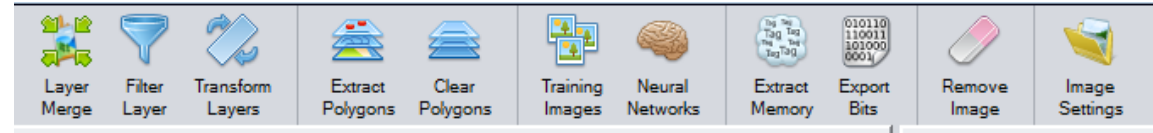
✓ Alignment Tab:

- Use stitch/stitch manager
- Move command used for manual alignment
- Add anchor define the positions that are aligned together
- Moving and static layer group define the reference layer and moving layer



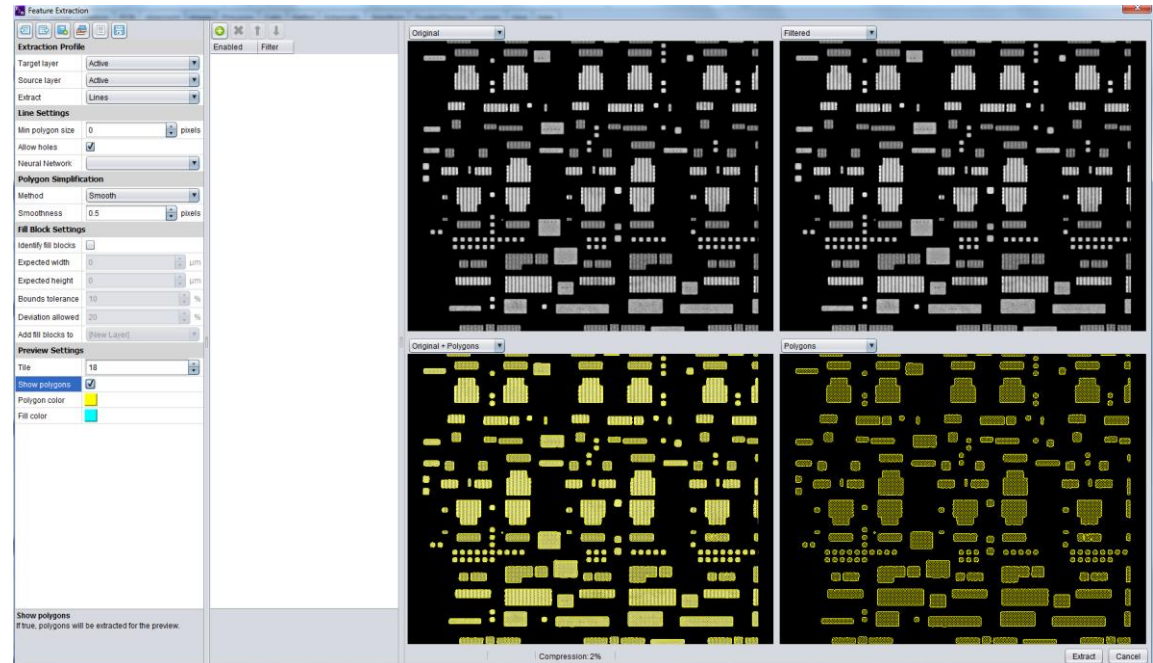
The image shows a dialog box titled 'Anchor Groups' with a table listing moving and static layers. The table has two columns: 'Moving' and 'Static'.

Moving	Static
M1	CA
Polysilicon	CA
CA	
Active	Polysilicon
Via 1	M1
M2	Via 1
M3	M2
M4	M3
M5	M4
M6	M5
Via 6	M6
M7	M6
M8	M7



✓ 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**

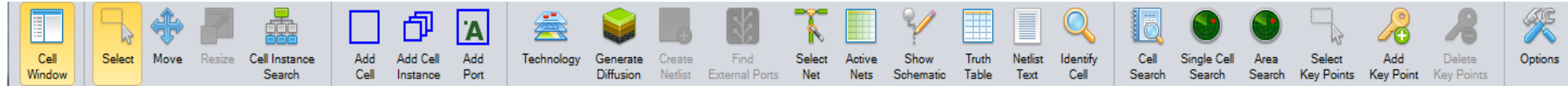
- Manual correction of polygon
- For analysis we will go for digital logic block 1 BUF 270.

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

- Pixel Transforms
 - Brightness
 - Contrast
 - Invert
 - Histogram Equalization
- Thresholding Filters
 - Threshold
 - Otsu's Method
 - Connectivity Threshold
- Smoothness Filters
 - Median Blur
 - Gaussian Blur
 - Bilateral Filter
 - Sharpen
- Morphological Operations
 - Dilate
 - Erode
 - Open
 - Close

Process Flow



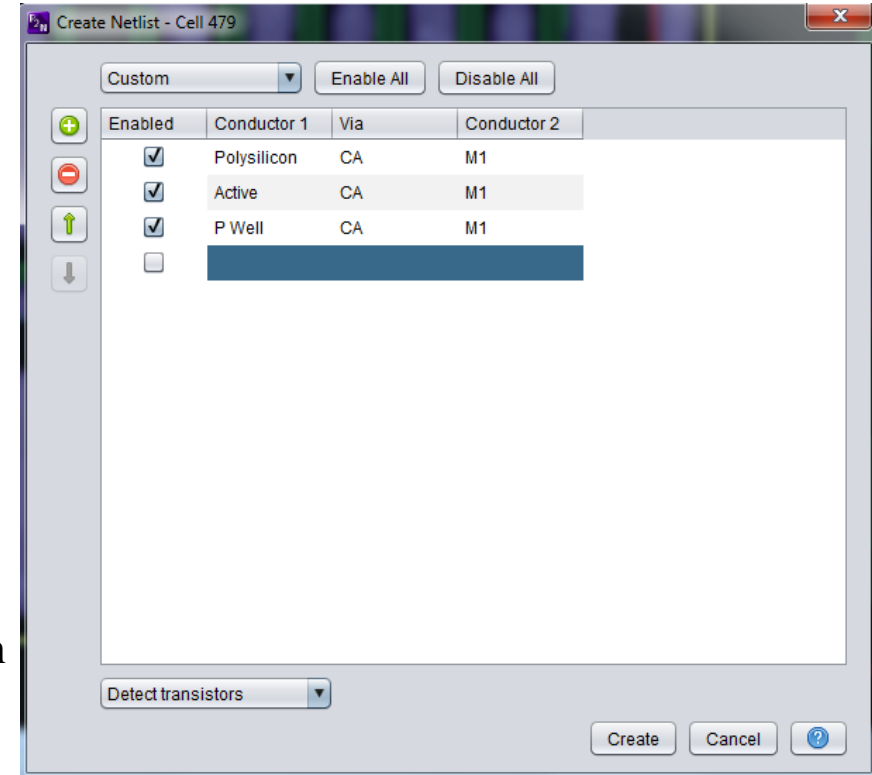
✓ Cell Tab:

- 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 technology create netlist command first.

BUF 270.



Question & Answer

