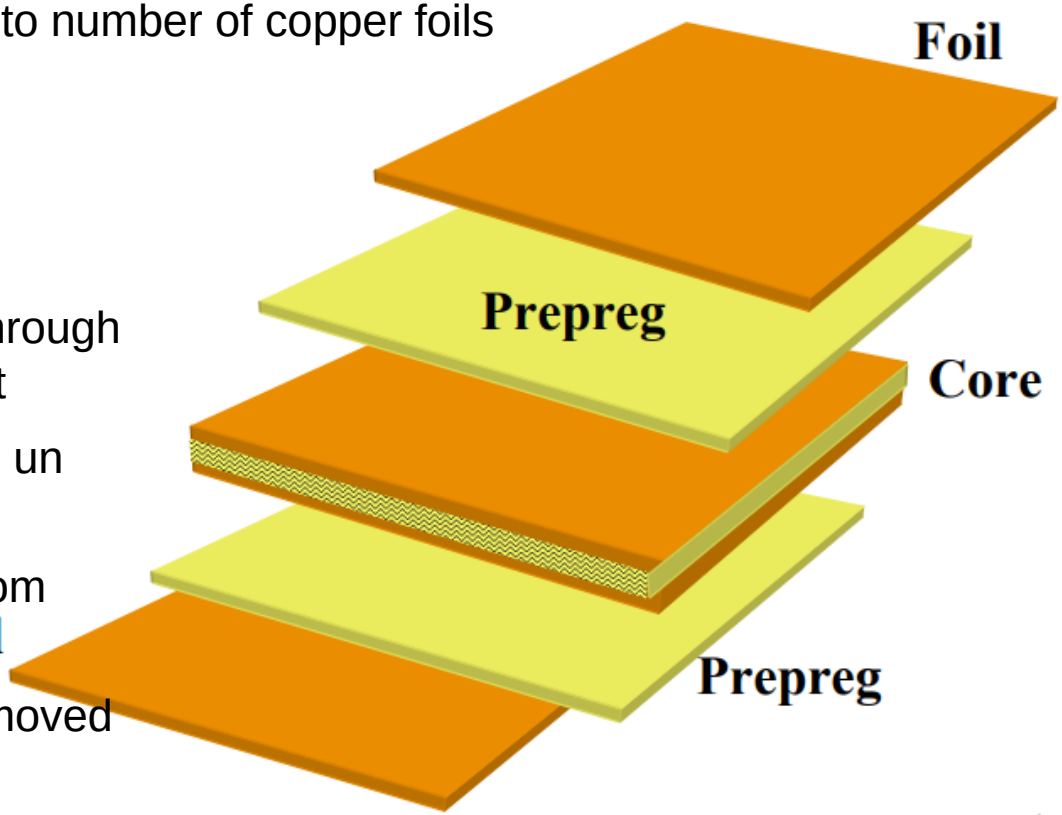
Anti RE

Navid Asadi

Physical Inspection and AttacKs on ElectronicS (PHIKS)

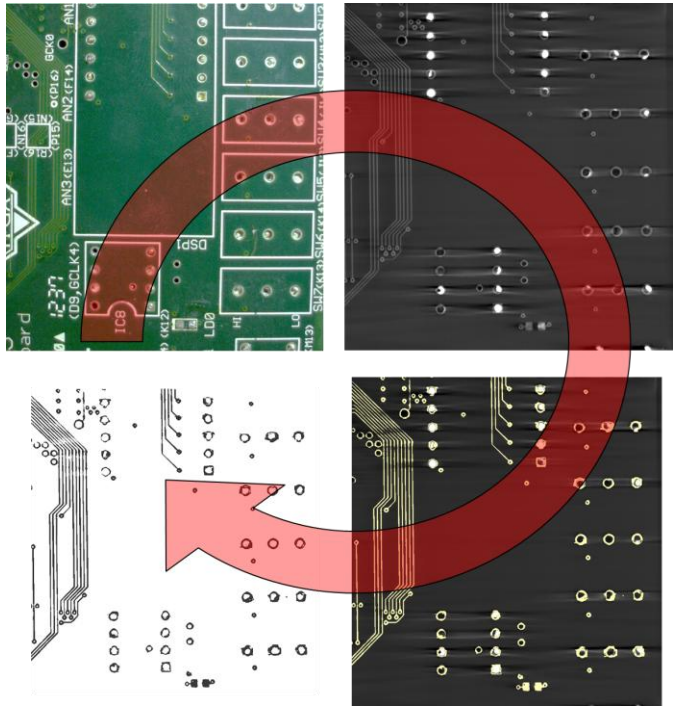
PCB Fabrication

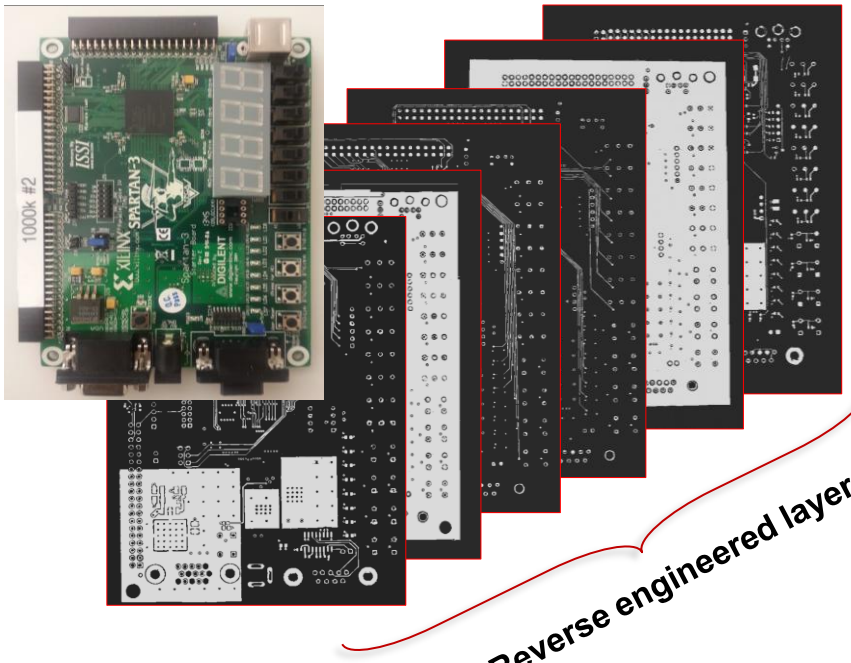
- Single layer
  - Glass epoxy core with copper foil on both sides
- Multi Layer
  - Same inner layer core with copper foil
  - Number of layers corresponds to number of copper foils
- Trace, pad deposition
  - Dry film resist coating
  - Gerber files printed on films
  - High intensity ultraviolet light through the film to polymerize the resist
  - Chemical solution removes the un polymerized regions
  - Copper removed chemically from uncovered areas
  - Dry film resist is chemically removed



Non-Destructive PCB Reverse Engineering

- **Tomography parameters are *optimized* for better PCB imaging**
- **X-ray images are successfully *denoised* and *segmented* using *localized thresholding***

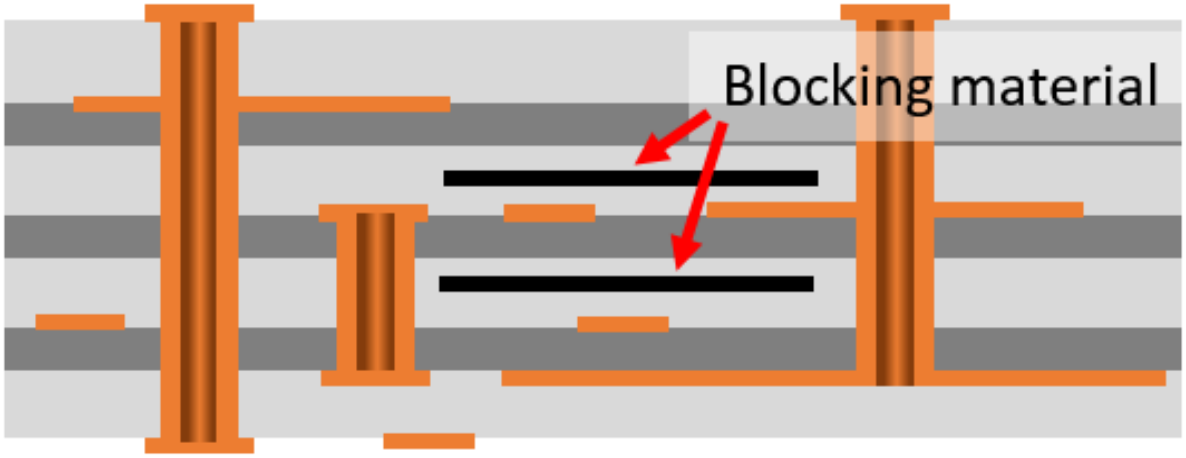




- **Segmented images are *stitched* to create a single file for each PCB layer.**
- **DXF files are generated from the segmentation output which can be directly converted to GERBER files for PCB printing.**

Potential Solutions

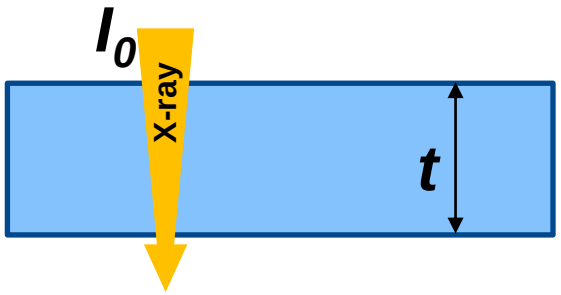
- Add blocking material to increase noise level on 2D projections.
- X-ray attenuation coefficient is dependent to the material physical density and atomic number
- Positioning high Z material next to low Z material can cause high noise level on the image data of low Z material
  - Higher X-ray power is required to transmit through the sample.
  - Low Z material are transparent against high Kv X-ray.



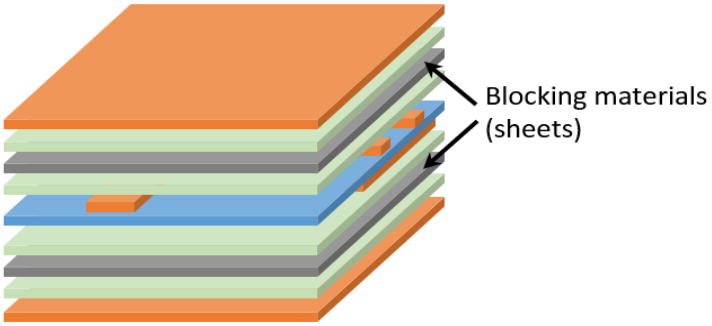
PCB with implemented blocking materials (high-Z material)

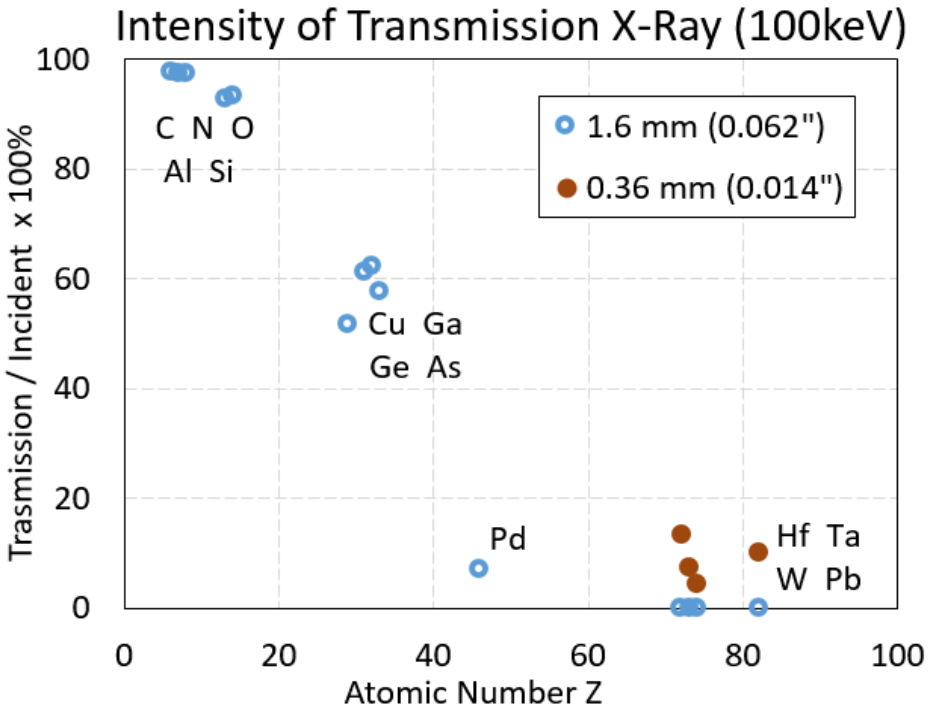
X-Ray Absorption Calculation

- The X-ray intensity depends on attenuation coefficient, mass density, and thickness of material elements.



$$I_t = I_0 \cdot \exp(-\frac{\mu}{\rho} \cdot \rho \cdot t)$$

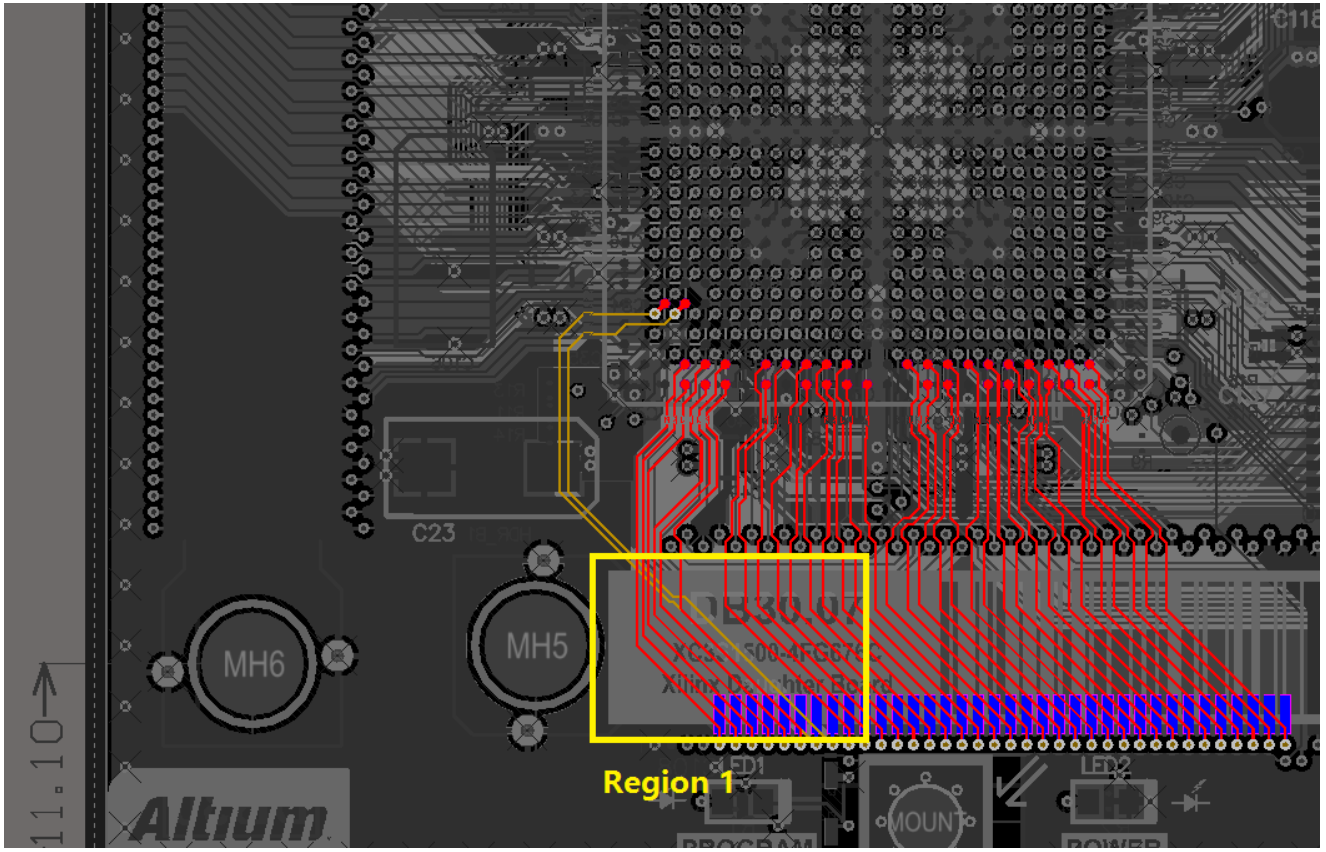




- High Z material can be added as: extra layers during PCB fab or particles mixed into resin-based prepreg for PCB bounding layers,
- Surface isolation might be necessary.

Trace Permutation

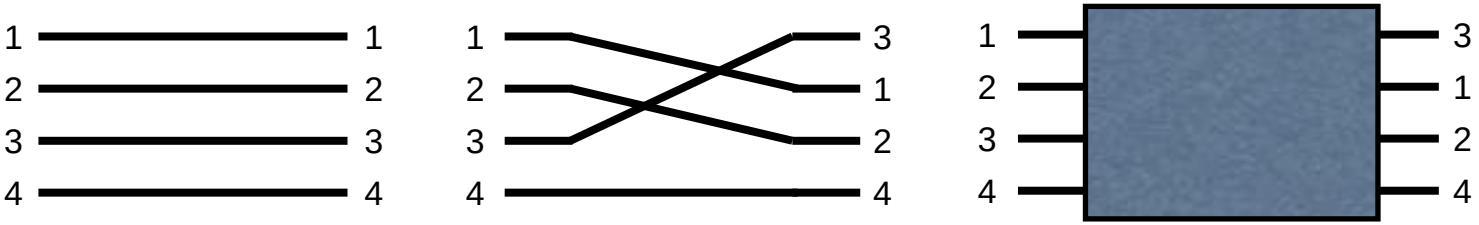
- Select a PCB region for blocking with high-Z material.



- The traces must be permuted.

Trace Permutation

- **Objective: permute the inter-chip connections within a mystery.**

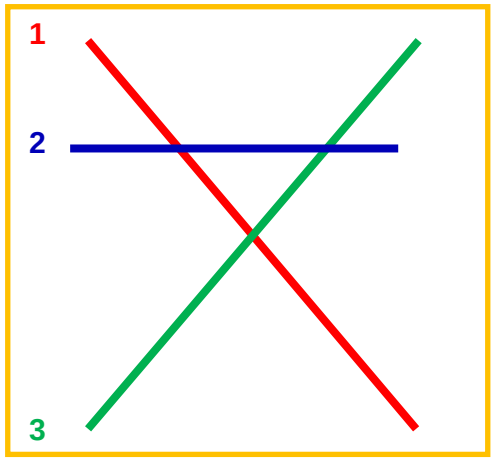


(a) Original design → (b) Internal trace permutation → (c) Cover with High-Z material

- **Parameters and metrics:**
  - **Numbers of inputs/outputs permuted (m/n).**
  - **Numbers of layers added (l).**
  - **Numbers of combinations (c).**
  - **Area overhead increased (a).**
- **Goals:**
  - **Goal 1: $f(m, n, c_{10}) = l$ (how many layers needed for certain I/O combination)**
  - **Goal 2: $f(m, n, l) = c$; $f(m, n, l) = a$**

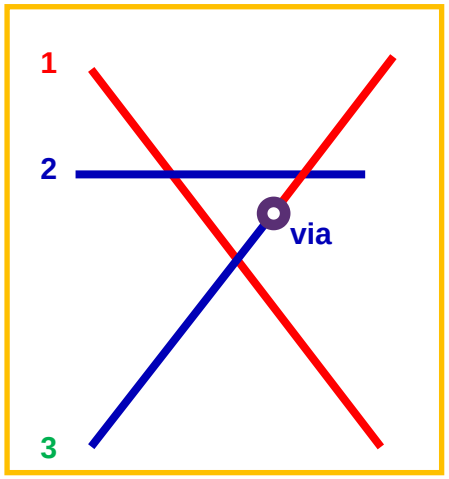
Assumptions

- **Without optimization:**
  - When the third trace intersect with two traces from different layers, an extra layer is needed.



  - This assumption is more general and requires less human effects.

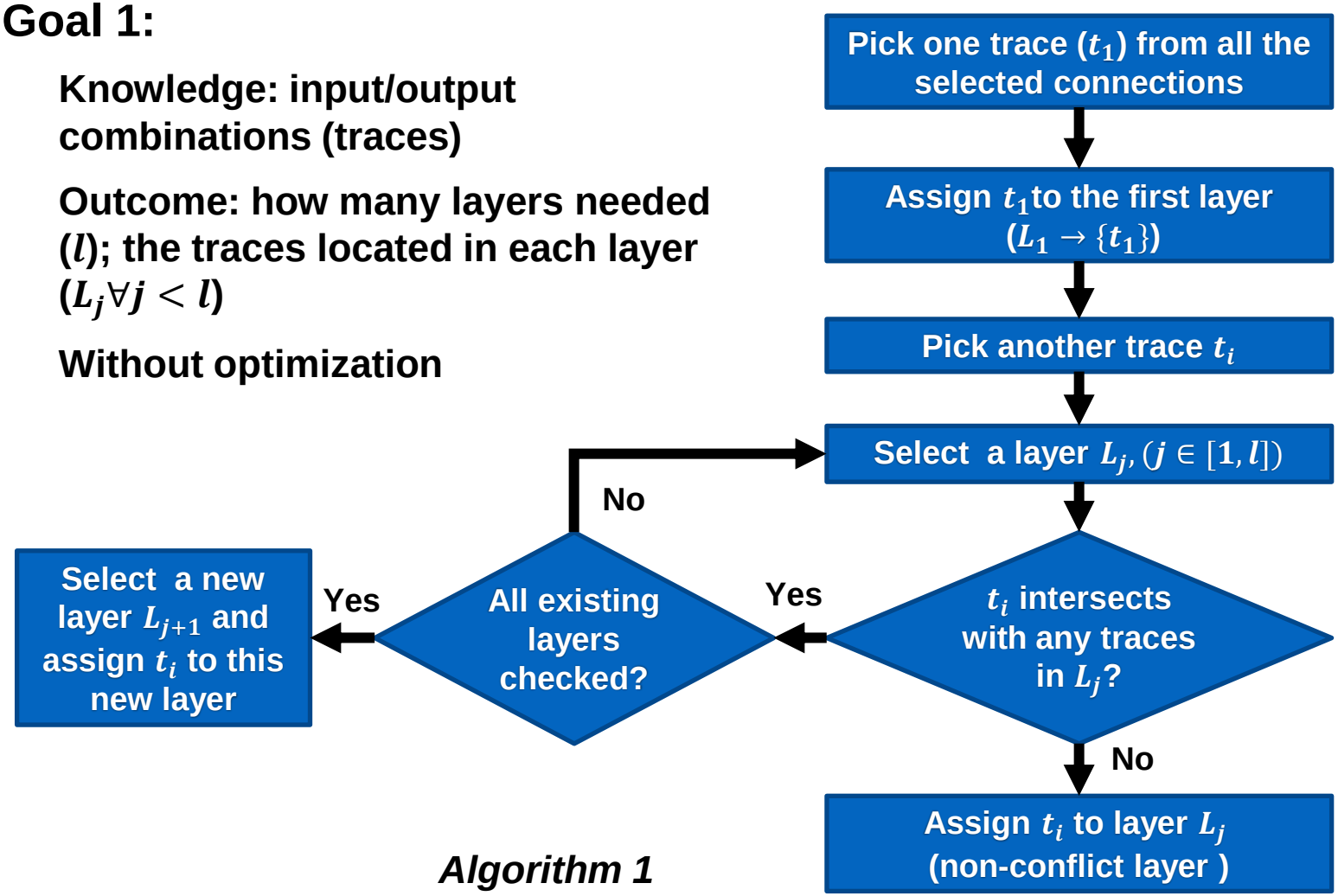
- **With optimization:**
  - When the third trace intersect with two traces from different layers, it can be routed only in the two existing layers.



  - This assumption could decrease the number layers required. But it may violate design rule checkings.

Algorithms to Achieve goal 1

- **Goal 1:**
  - **Knowledge: input/output combinations (traces)**
  - **Outcome: how many layers needed (l); the traces located in each layer ($L_j \forall j < l$)**
  - **Without optimization**

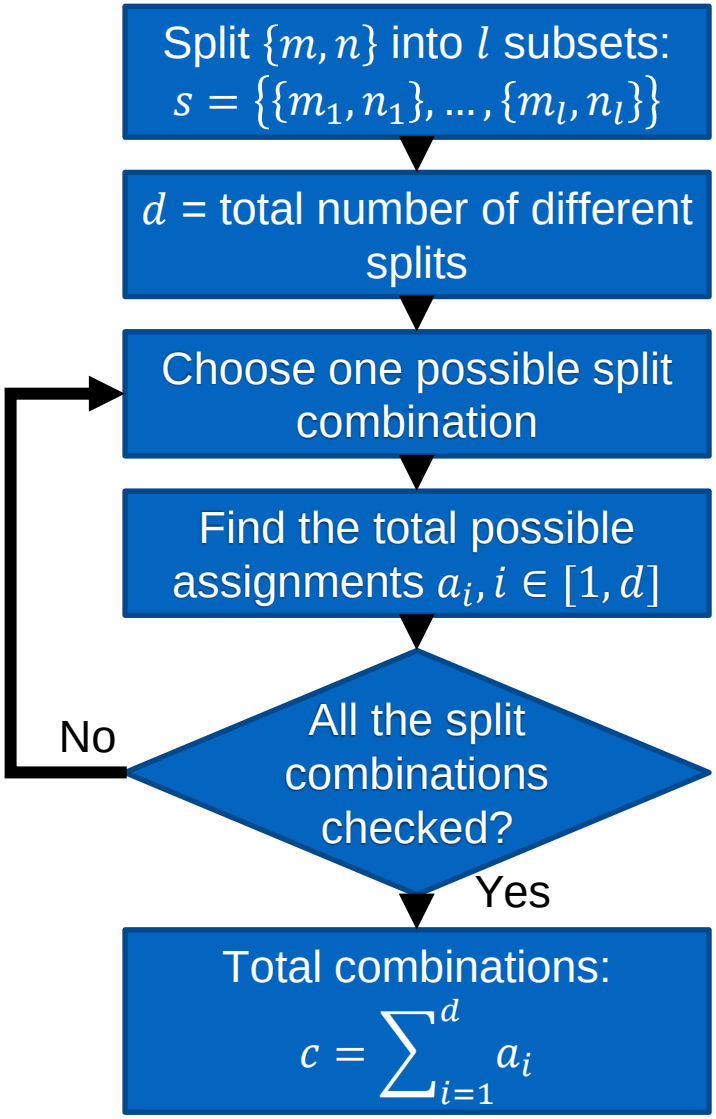


Algorithm 1

Algorithms to Achieve goal 2

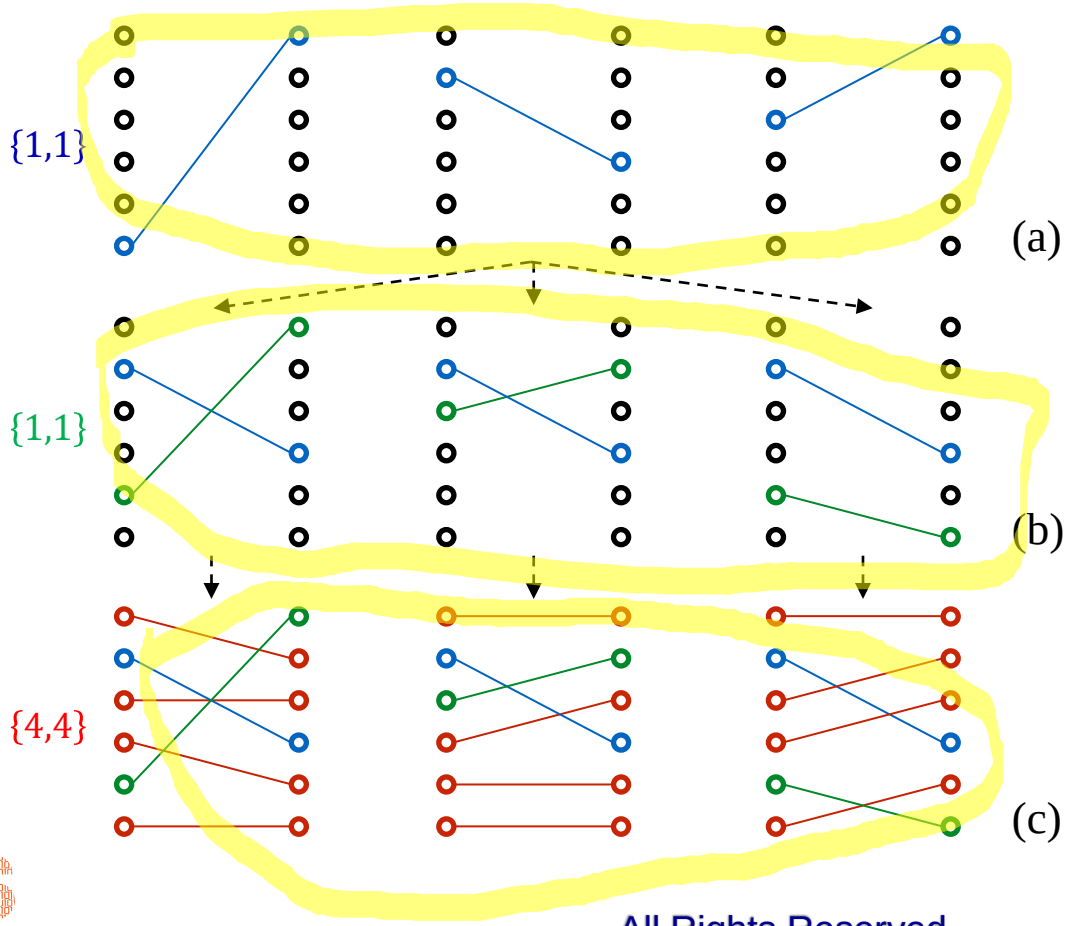
- **Goal 2:**
  - **Knowledge: input/output numbers (m/n), number of layers allowed (l)**
  - **Outcome: number of combinations (c)**
  - **Without optimization**

Algorithm 2



Example for Developed Algorithms

- **Algorithm 2 explanation** ($m = n = 6, l = 3$)
  - **Possible subsets** ($d = 3$):
    - $s_1 = \{\{1,1\},\{1,1\},\{4,4\}\}$; $s_2 = \{\{1,1\},\{2,2\},\{3,3\}\}$; $s_3 = \{\{2,2\},\{2,2\},\{2,2\}\}$



$$a_1 = a_{1,1} \times a_{1,2} \times a_{1,3}$$

(a) $a_{1,1} = 6 * 6 = 36$

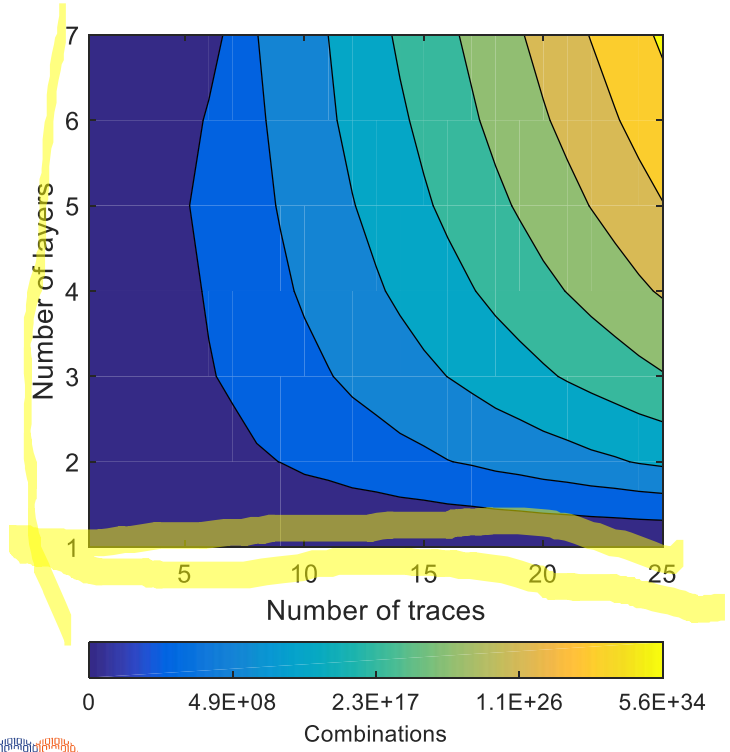
(b) $a_{1,2} = 5 * 5 = 25$

(c) $a_{1,3} = 1$

c calculation results

Setups:

- $m = n$
- Number of layers: 2 to 7
- Number of traces: 5 to 25



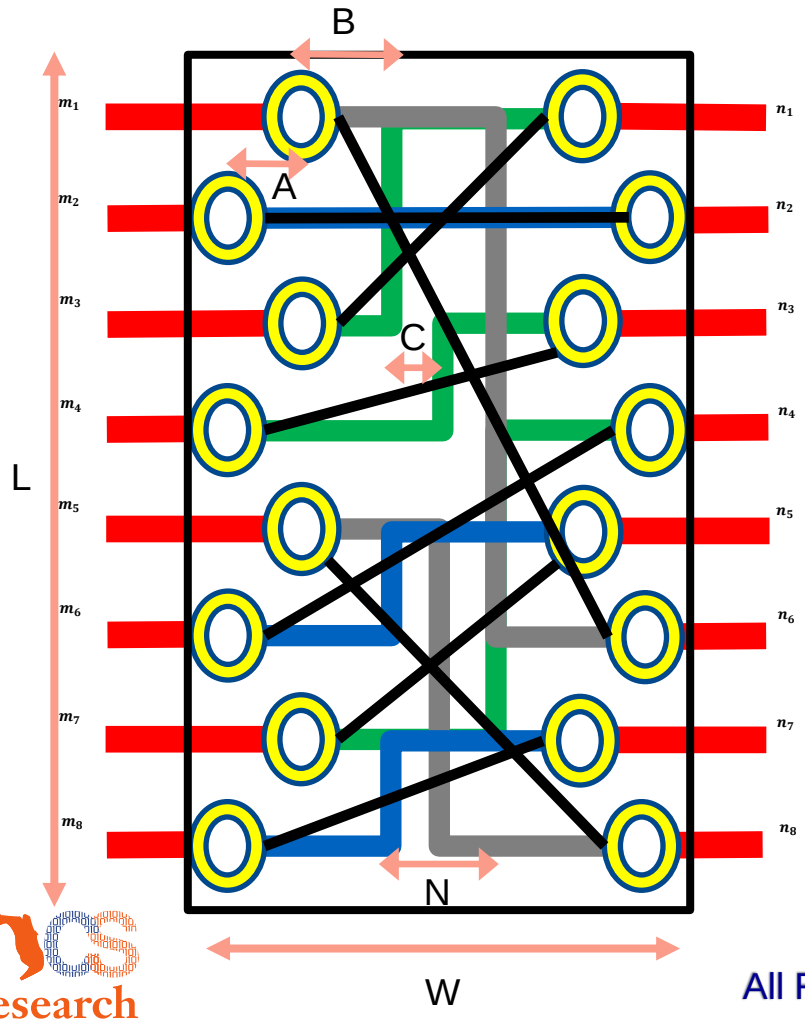
Reference names

- 1. DB30 Xilinx Spartan-3 FGG676
- 2. SL1 Xilinx Spartan-IIE PQ208
- 3. NBP3 Altera MAX7000 MAX3000 PLCC
- 4. NanoBoard-NB2DSK

Performance evaluation.				
Design No.	Input/ output (m/n)	Middle layers (l)		Comb. (c)
		Require	Actual	Total
1	16/16	3	4	1.2e+13
2	14/14	3	0	1.7e+11
3	18/18	3	0	9.3e+14
4	19/19	3	4	7.1e+15

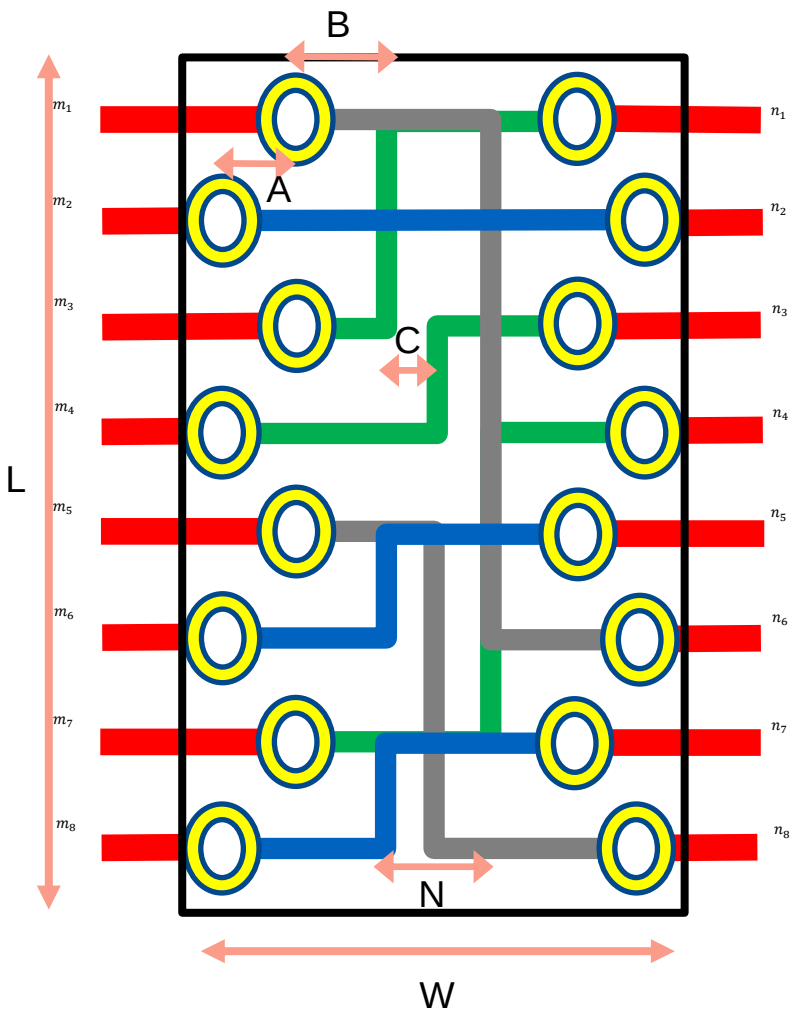
Area Overhead Estimation for Permutation Network

- Staggered vias
  - Spaced according to minimum design rules
  - Allows wires to be routed to different layers



- Permutation network
  - Assign layers to wires such that they do not cross in a single layer
- Route wires with minimum spacing in their respective layers
- Calculate resulting area (L * W) based on
  - A (Via to via spacing)
  - B (Via to track spacing)
  - C (Track to track spacing)
  - N (number of track to track gaps * track to track spacing)

Area Overhead Estimation for Permutation Network

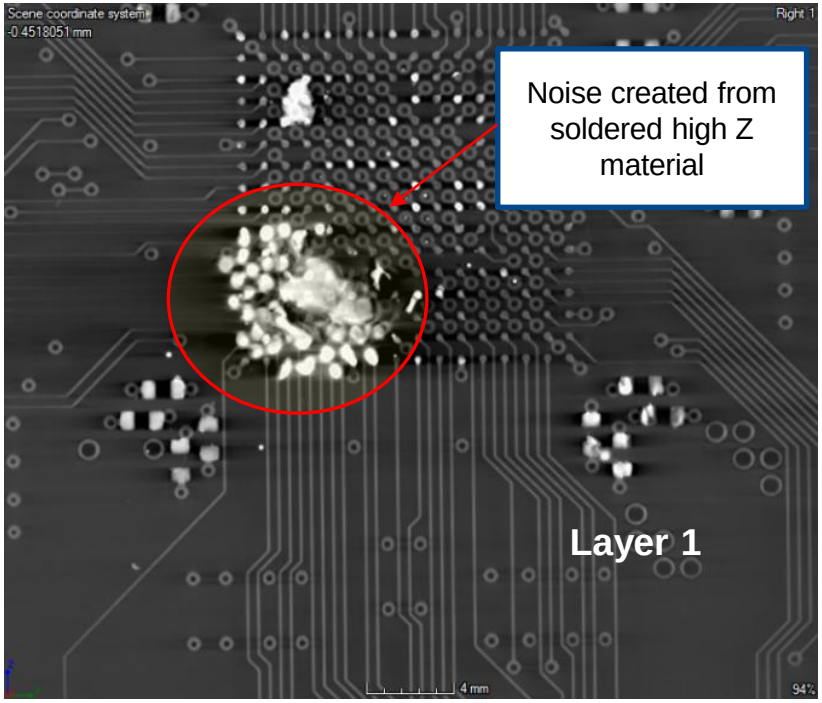


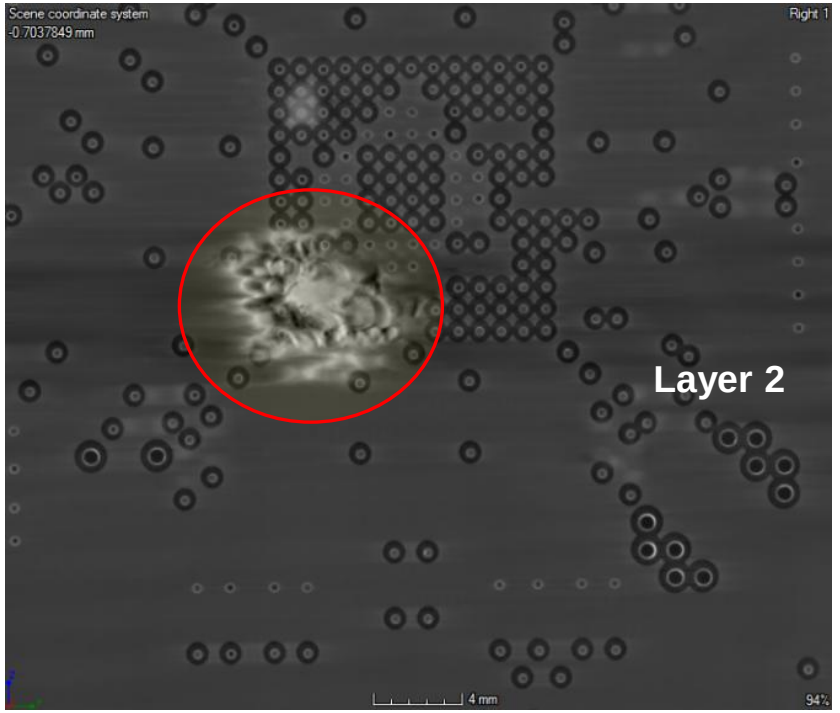
Design No.	Input/ output (m/n)	N	Area (W x H) / mm^2	% Area of Total PCB Footprint
1	16/16	5	106.41 (6.26 x 17.01)	1.14
2	14/14	4	85.60 (5.74 x 14.92)	0.94
3	18/18	6	129.40 (6.77 x 19.10)	2.31
4	19/19	5	126.05 (6.26 x 20.15)	2.55

- **Via diameter, via-via, via-track, track-track distance from Advanced Circuits, AZ (4PCB)**
- **Used random permutations and determined avg. N (no. of track-track gaps needed to do routing)**
- **Less than 130 $\mathbf{mm^2}$ of PCB footprint**

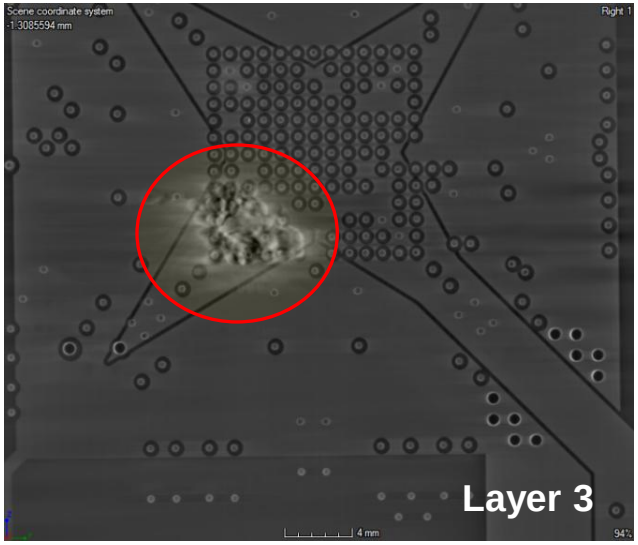
High-Z material blocking

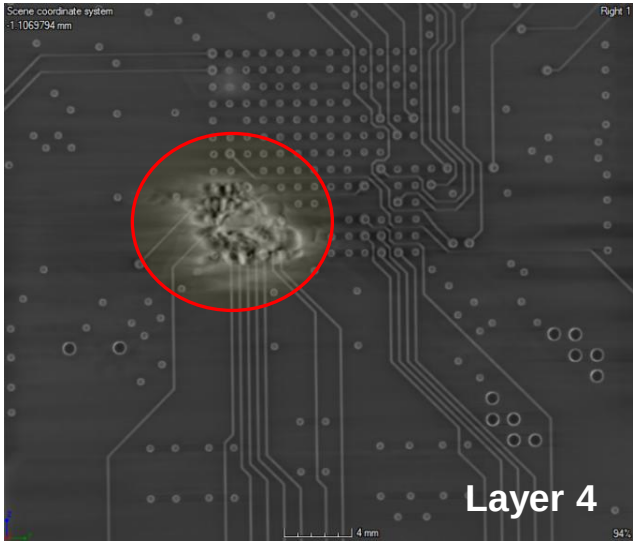
- **Atomic number for these high-Z materials is in the range of 70–80.**
- **It is higher than the atomic number of copper (29) or aluminum (13).**
- **The high-Z materials can cause major shadowing and noise on the results.**

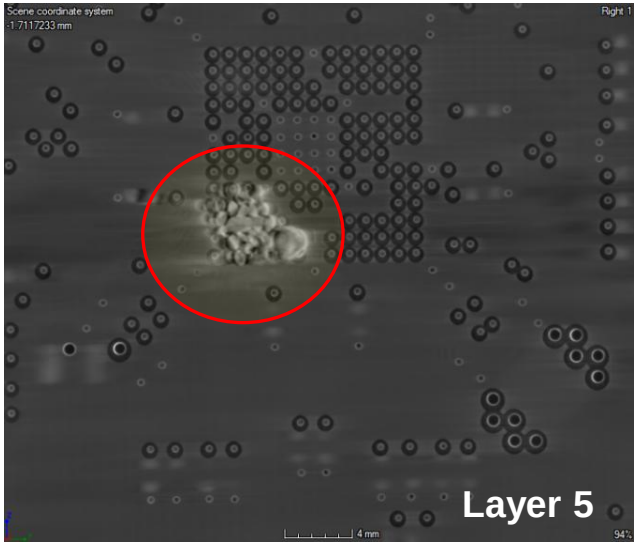


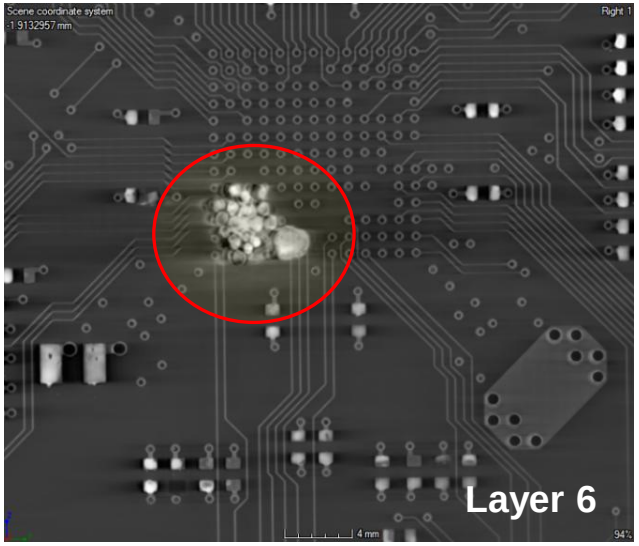


High-Z material blocking





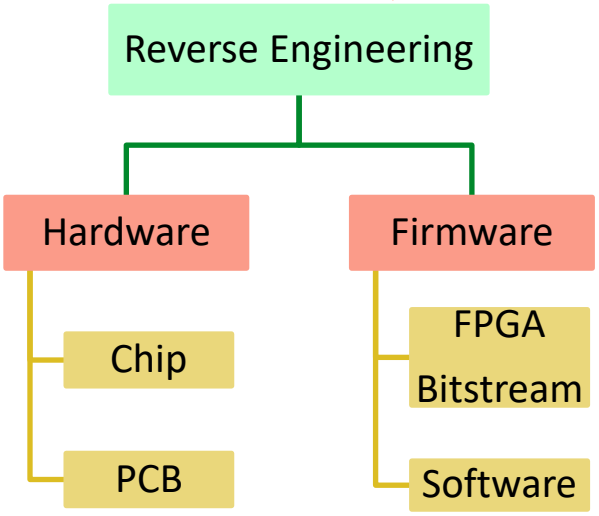




Reverse Engineering

Primary Purpose of RE

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



Chip Level RE

- ✓ 5 Steps for complete chip RE

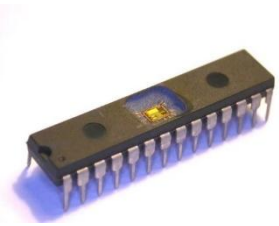
Imaging
- SEM/ Optical

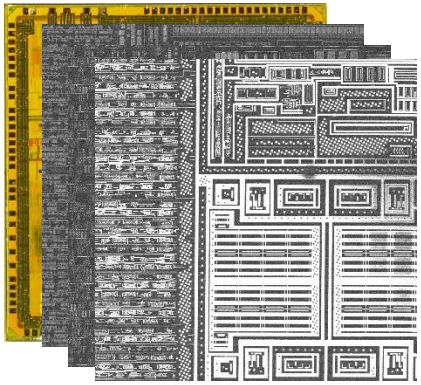
Depacakging
- Selective
- Non-selective
- Frontside
- Backside

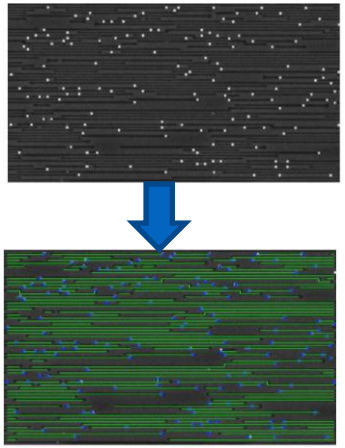
Delayering
- Plasma/FIB etching
- Wet etching

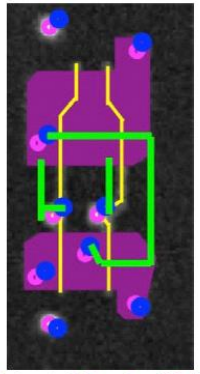
Annotation
- Extract Layer Information

Functionality
- Extract netlist
- VHDL code

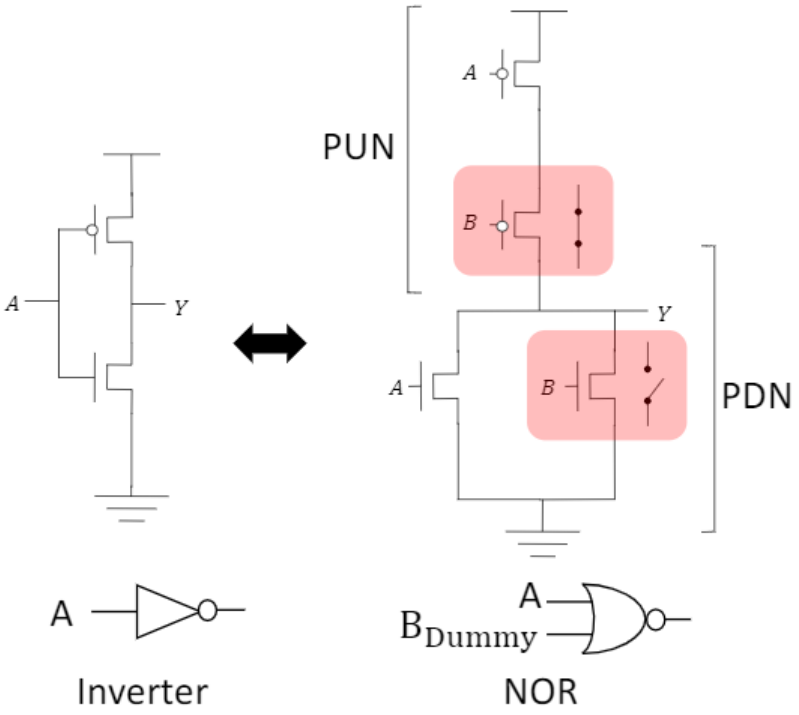








Anti Re ICs using Camouflaged Gates

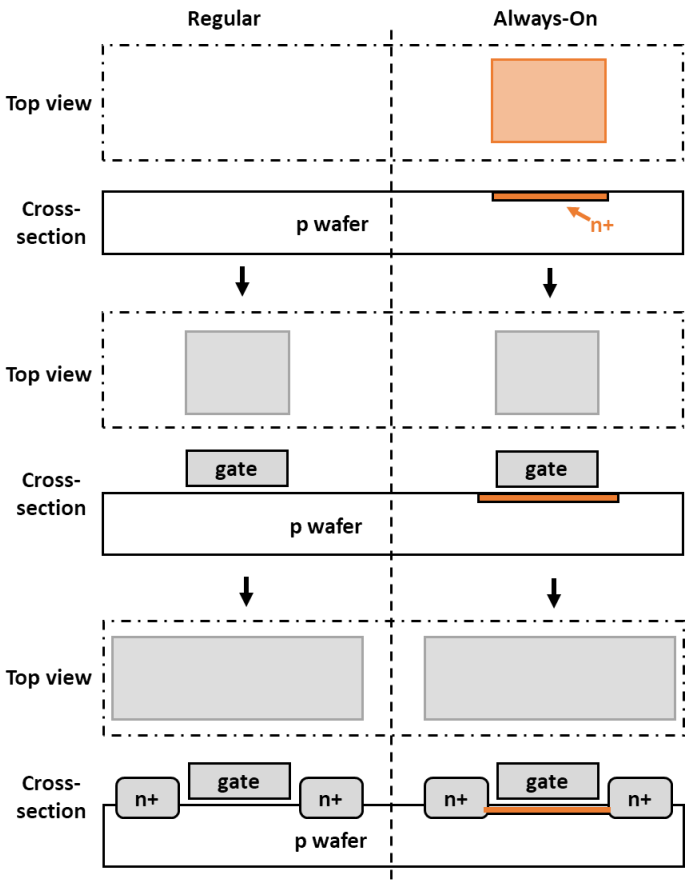


By insert an “Always-On” PMOS to PUN (pull-up-network), and an “Always-Off” NMOS to PDN (pull-down-network), an inverter appears as a NOR gate.

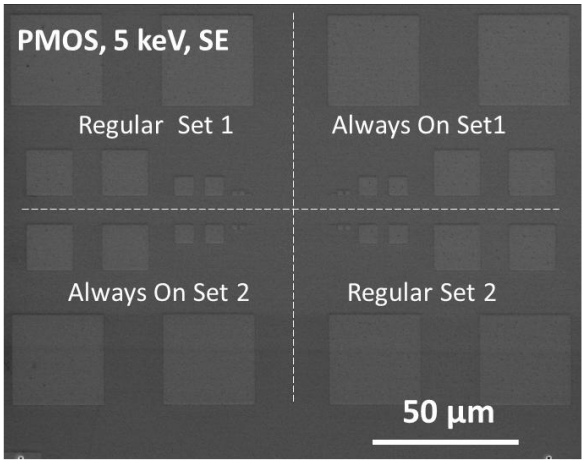
Under SEM, we want the modified invertor looks exactly like a NOR gate.

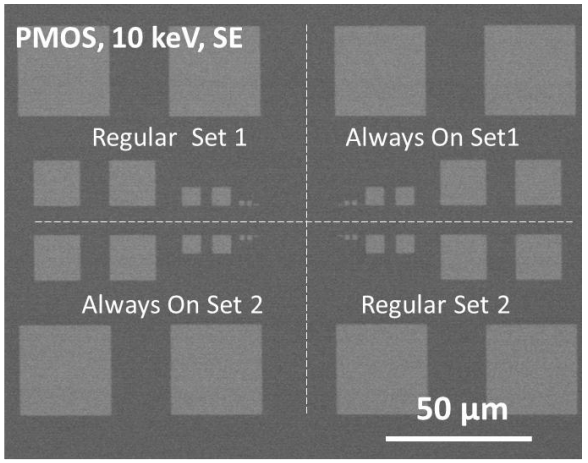
SEM Images – Always On Gates

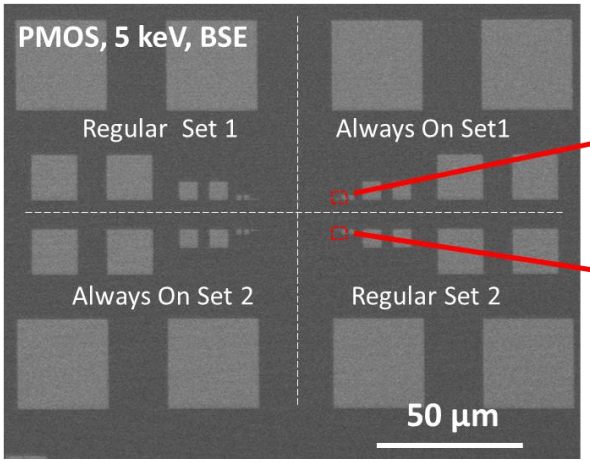
How to fab an “Always-On” gate

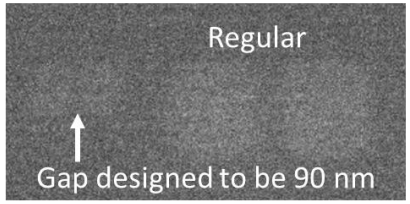


Regular transistors Vs “Always-On” transistors from front side
(only doped regions are fabricated, without gates and contacts.)



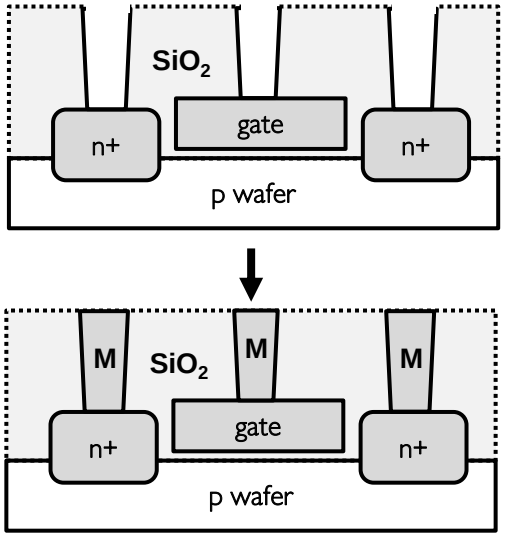




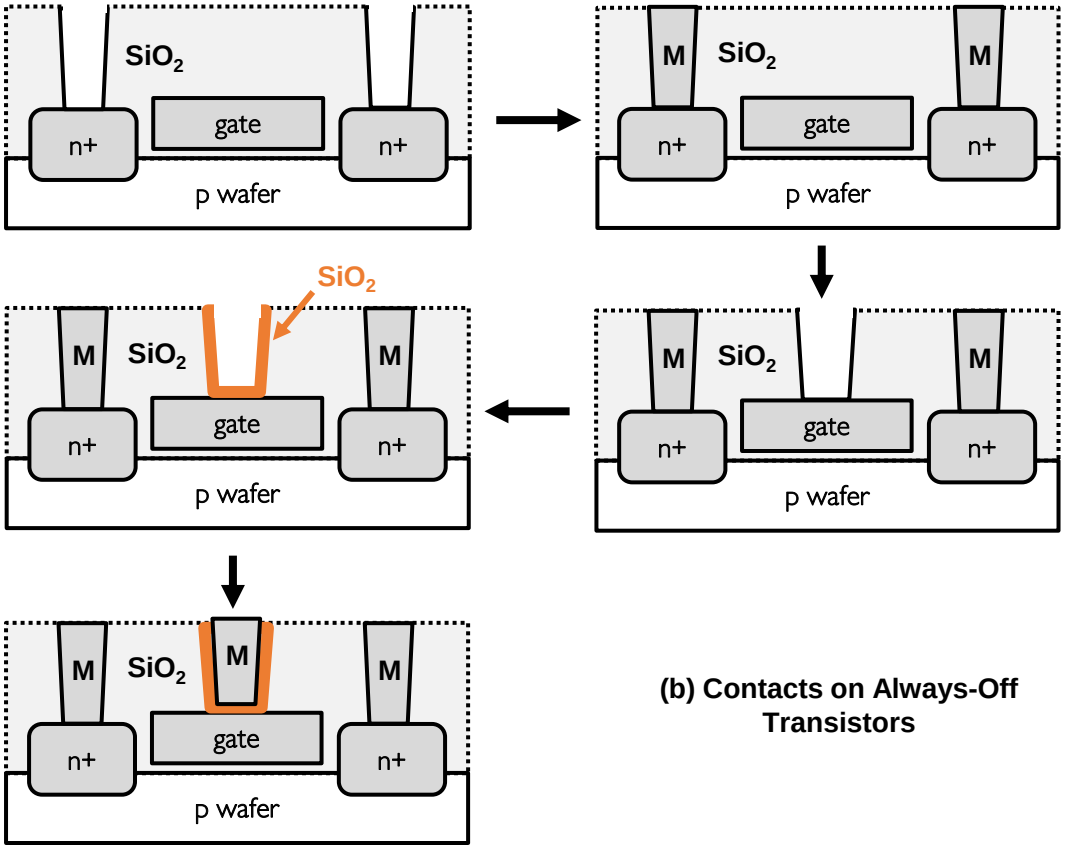


Always Off Gate

Using a dummy contact on gate

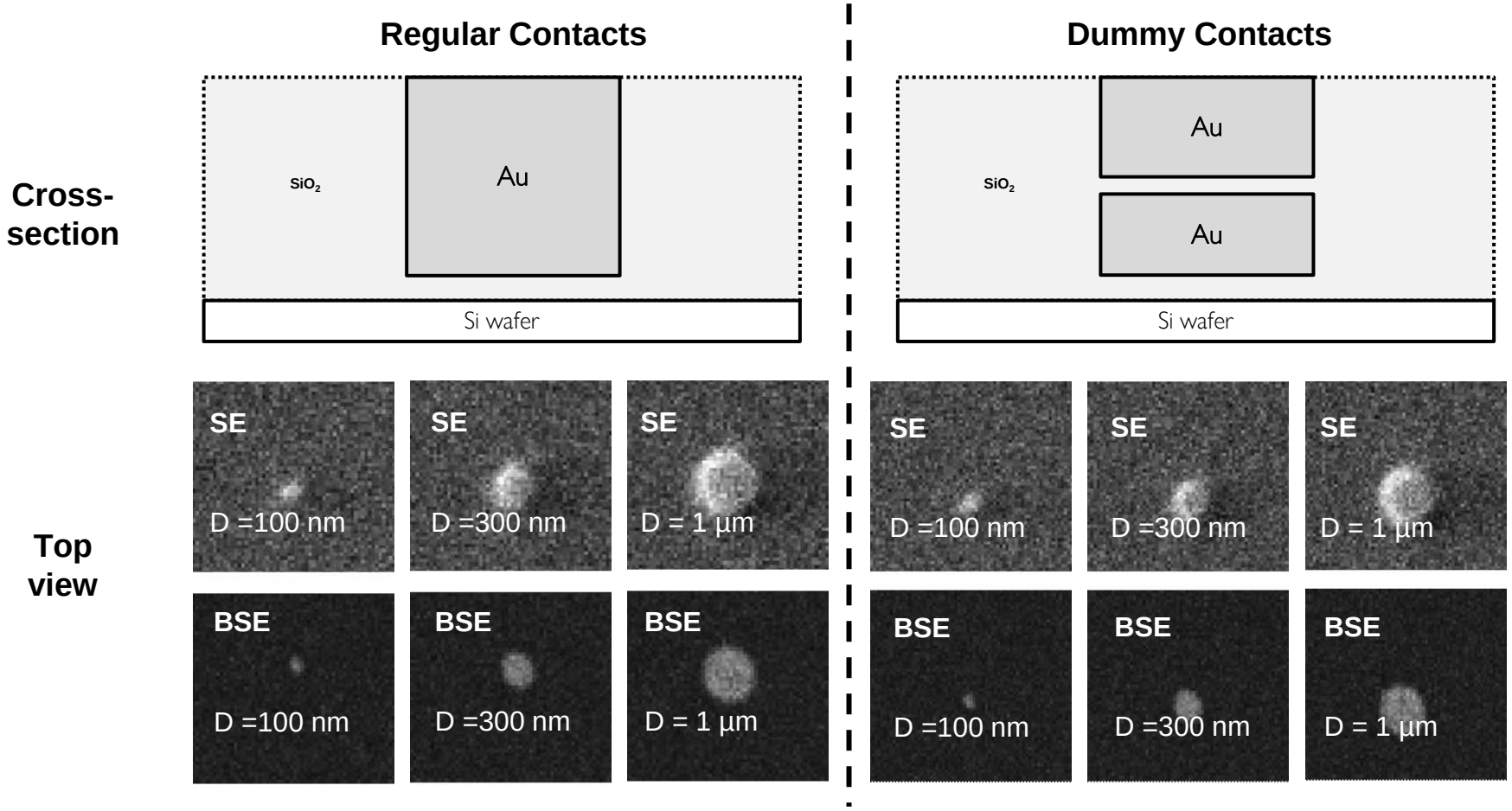


(a) Contacts on Regular Transistors



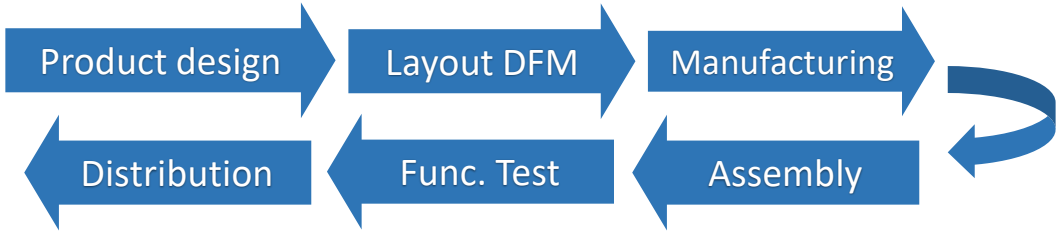
(b) Contacts on Always-Off Transistors

SEM Images – Always Off Gates



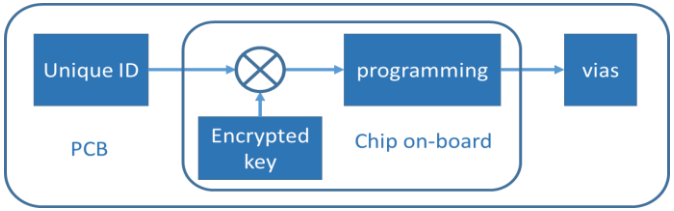
Vanishing Connections

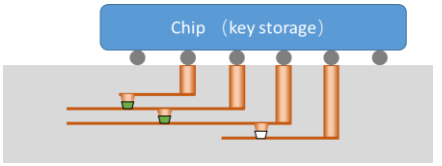
- Camouflaging-based Countermeasure against Reverse Engineering



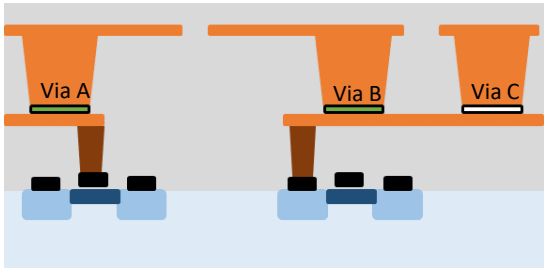
Hardware IP protection against:
1. **Post-fabrication reverse engineering**
2. **Piracy in untrusted foundries**

- **Private key: set up correct connections**
- **Key stored on board or given on usage**
- **Connections vanish when the board off**
- **Dummy connections for camouflaging**

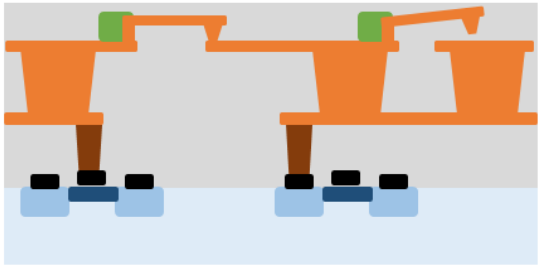




Programmable Memristor Visa



MEMS/NEMS Connections



Microfluid Connections