UCLouvain | RUHR UNIVERSITÄT BOCHUM | RUB | Bundeskriminalamt

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

RED TEAM VS. BLUE TEAM:

A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations

Endres Puschner, Thorben Moos, Steffen Becker, Christian Kison, Amir Moradi, Christof Paar

↘ *HARRIS'2023*

↘ *Wednesday, January 25th, 2023*

WHAT ARE HARDWARE TROJANS?

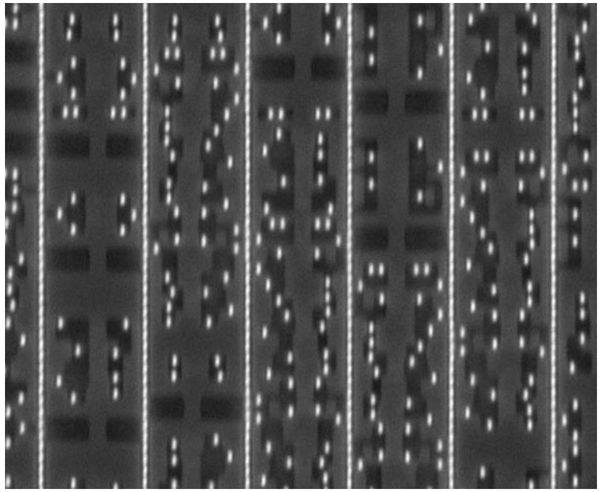
- Unwanted functionality in hardware
- Device functions as designed

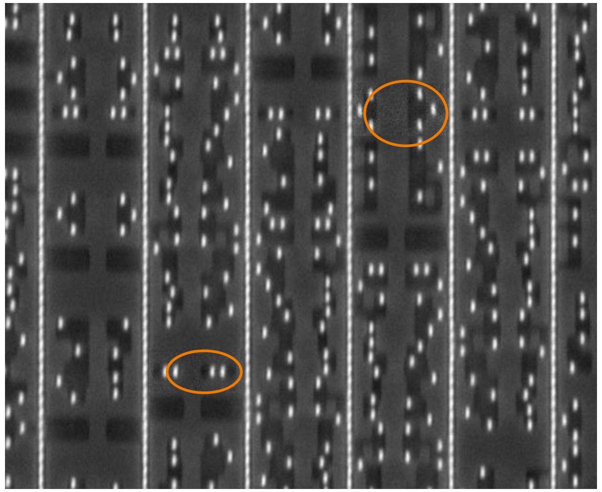
→ Here: Trojans that are physically realized by adding or modifying gates

- CMOS Integrated Circuits

Example

- Cryprographic Co-Processors
- Key / Algorithm Weakening



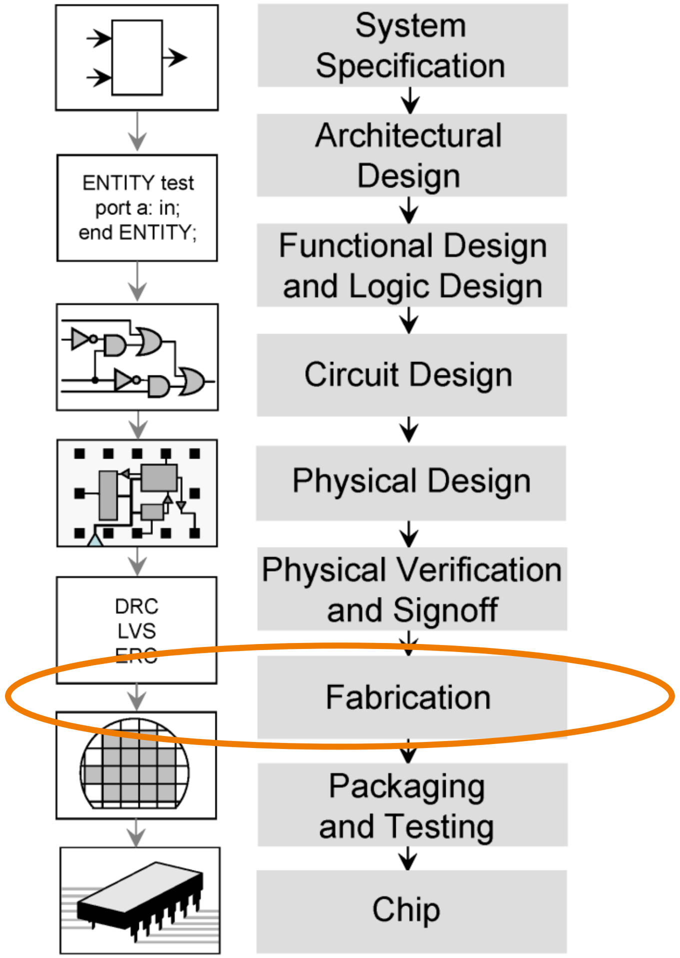


HOW CAN HARDWARE TROJANS GET INSERTED?

- Globalized supply chain

1. Designer sends GDSII design file to fab,
2. Fab produces physical masks and chips

- Many entry points for adversaries
  - Rogue employees
  - Subverted design tools
  - Malicious third-party IP cores
  - Intercepted transportation or untrusted contractor
  - **Untrusted fab**



Integrated Circuit Design, Linear77, CC BY 3.0, via Wikimedia Commons

THREAT MODEL

We consider the following scenario:

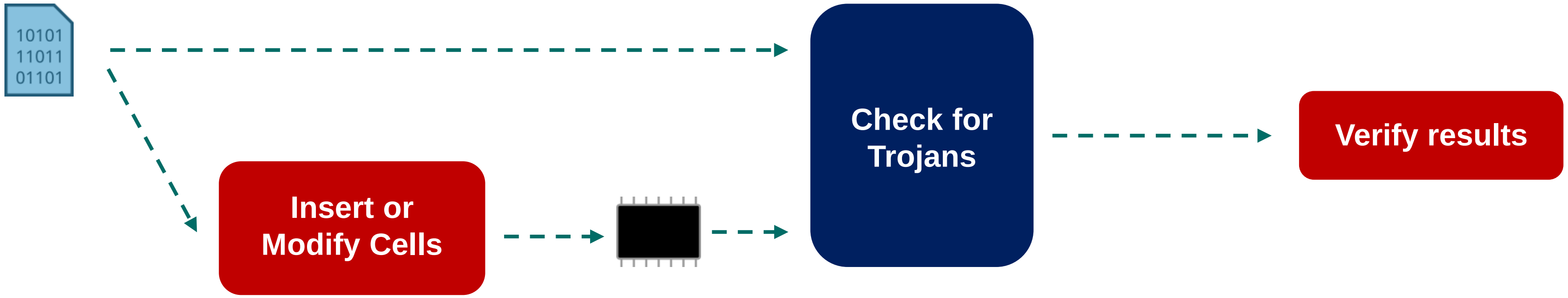
- Chip design leaving the IC design house is Trojan-free
- Threat is mainly manufacturing of the chips

Main Research Question: How efficiently can we detect functional hardware Trojans in full-sized ICs manufactured in progressively smaller CMOS technologies?

- We employ a Red Team vs. Blue Team approach to enable an independent and realistic assessment

OUR APPROACH

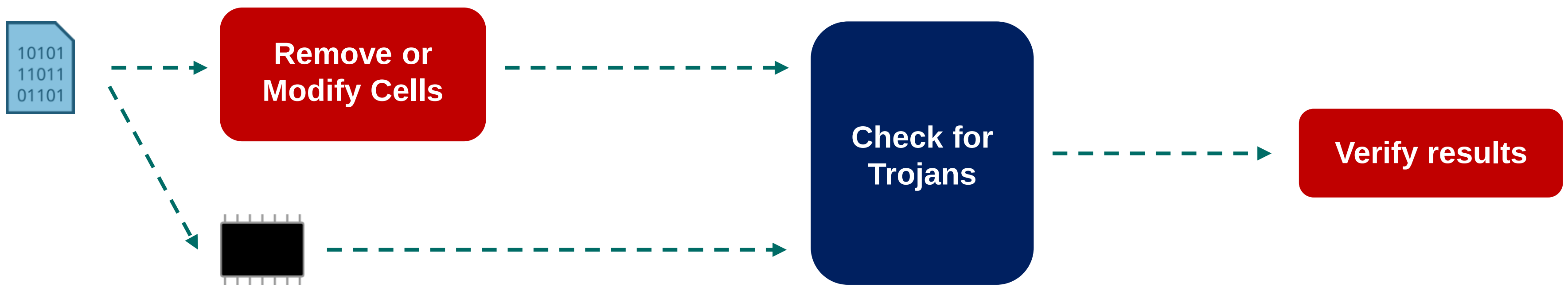
- Blue Team (analysis lab) receives chips prepared by the Red Team (malicious fab)
- Task of the Blue Team is to find inserted / replaced cells in the real chips not matching the design file
- Mismatches get reported to the Red Team and thus are verified
- Research bias minimized



OUR APPROACH

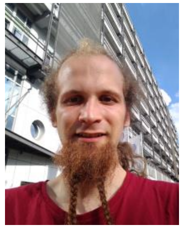
design files

- Blue Team (analysis lab) receives ~~chips~~ prepared by the Red Team (malicious fab)
- Task of the Blue Team is to find inserted / replaced cells in the real chips not matching the design file
- Mismatches get reported to the Red Team and thus are verified
- Research bias minimized



- Better for us!

THE TEAM

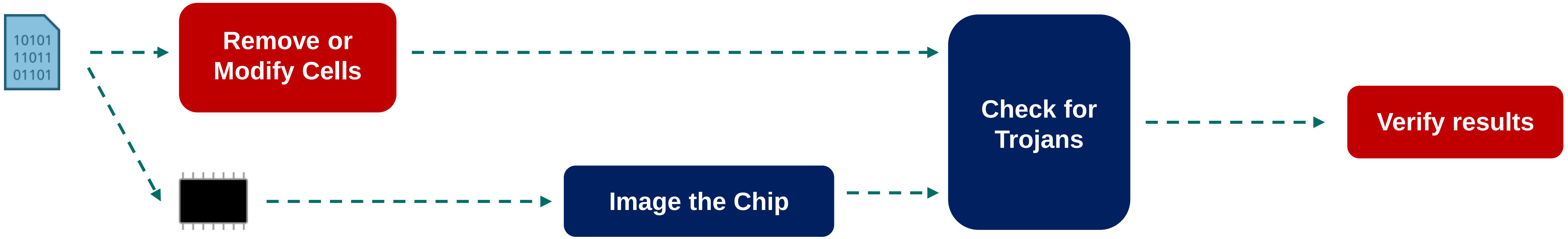
    

Thorben Moos

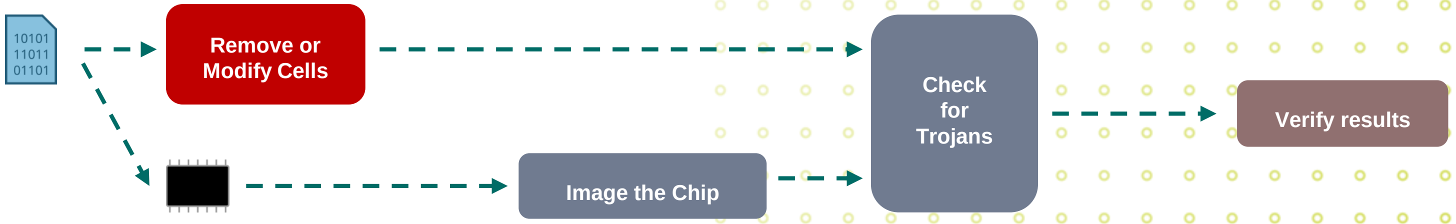
Christian Kison

Endres Puschner,
Steffen Becker

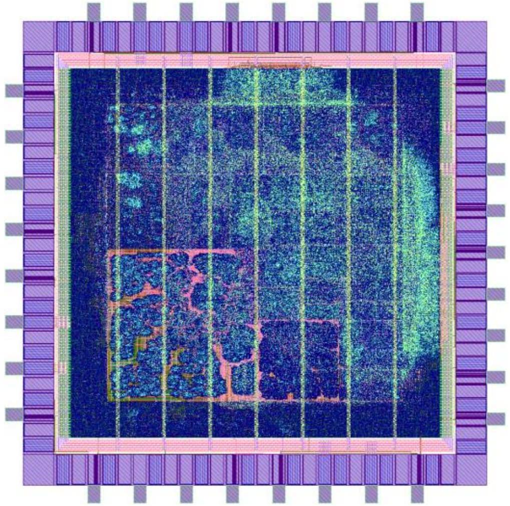
Thorben Moos



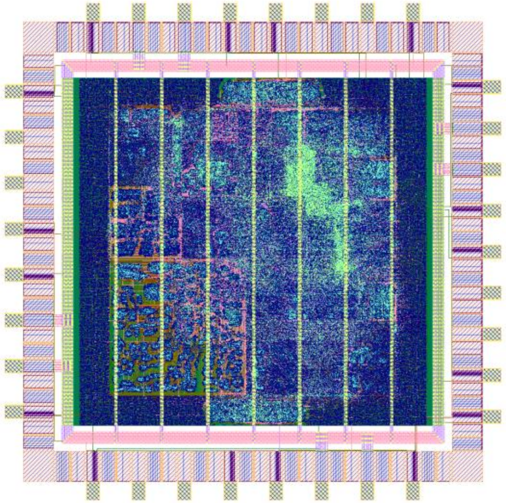
RED TEAM: REMOVE OR MODIFY CELLS



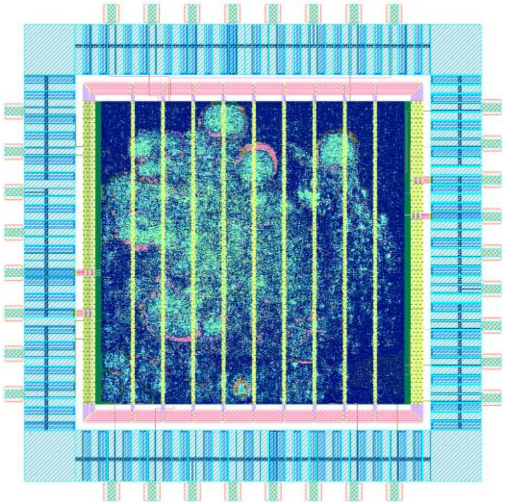
THE CHIPS



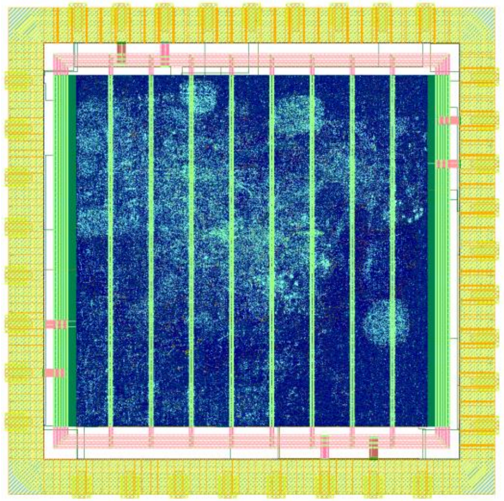
a) 90nm ASIC



b) 65nm ASIC



c) 40nm ASIC

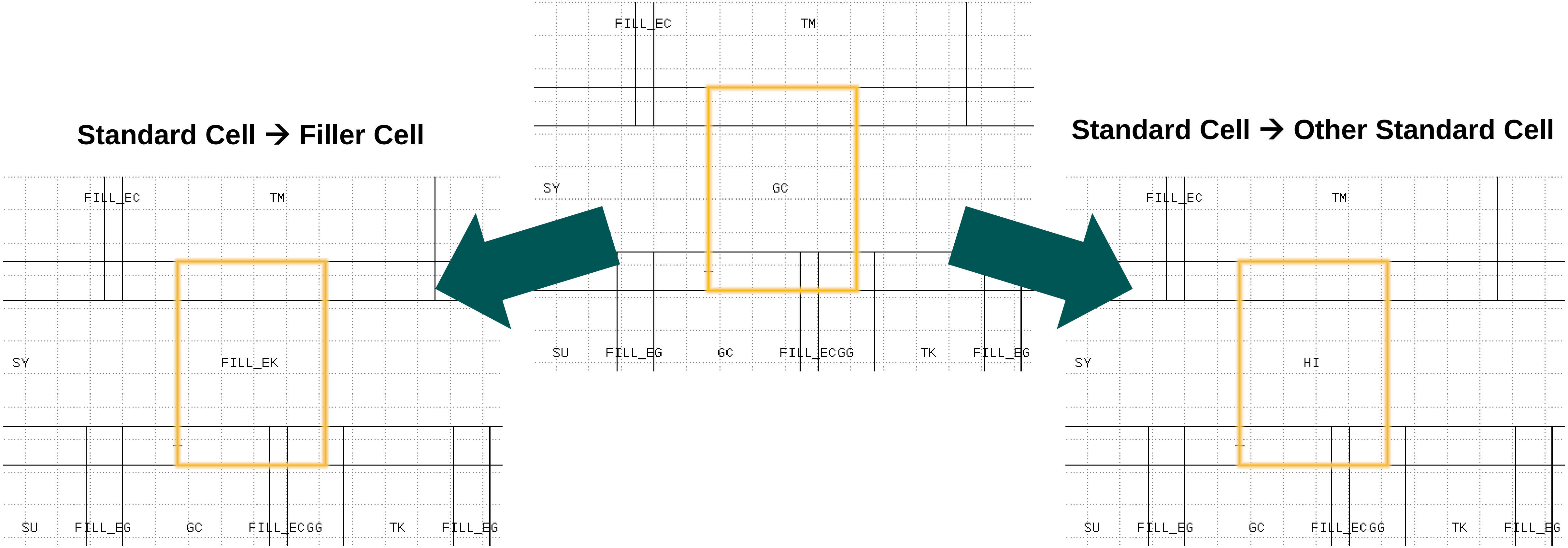


d) 28nm ASIC

TROJAN INSERTION

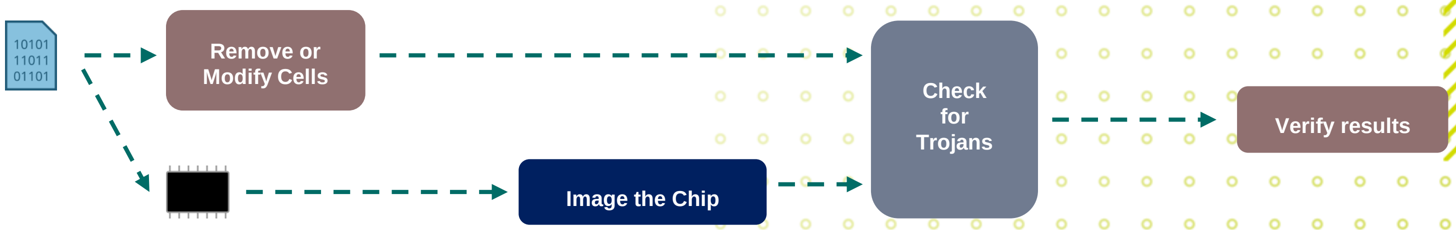
Standard Cell → Filler Cell

Standard Cell → Other Standard Cell

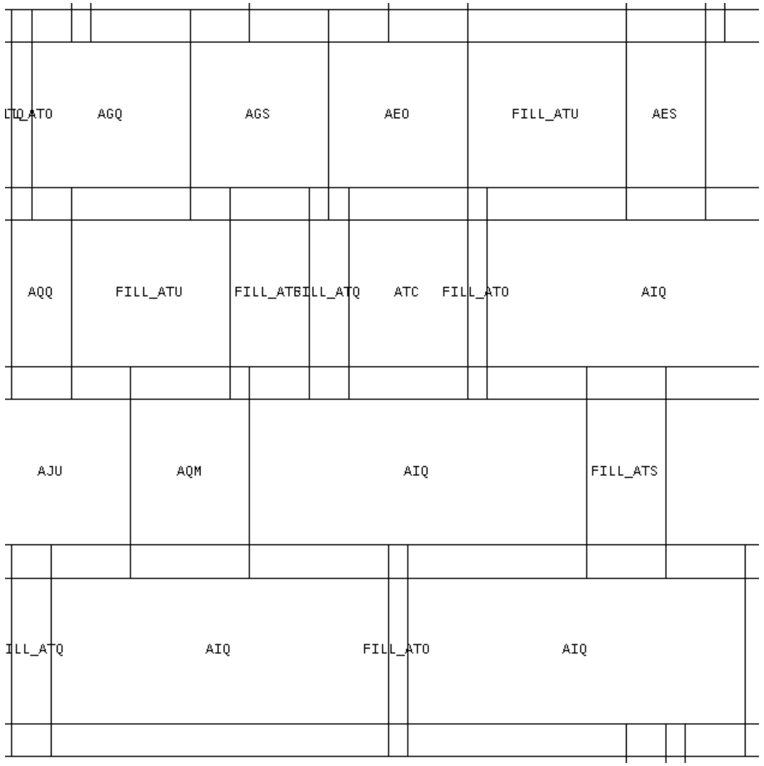


- Modifications are chosen at random positions
- Scattered over the chip area

BLUE TEAM: IMAGE THE CHIP



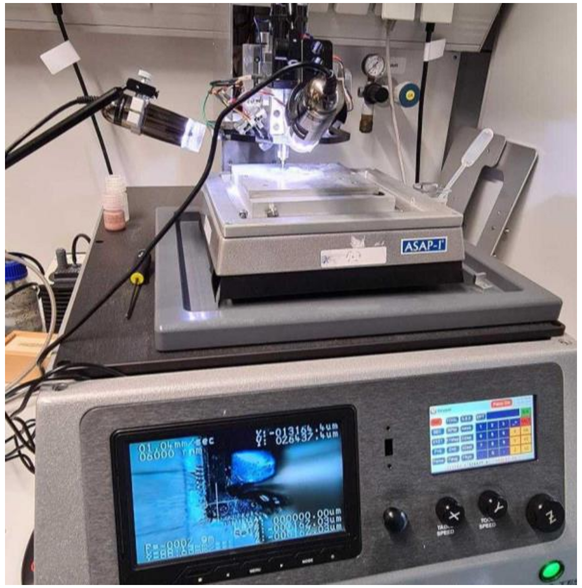
BLUE TEAM RECEIVES:



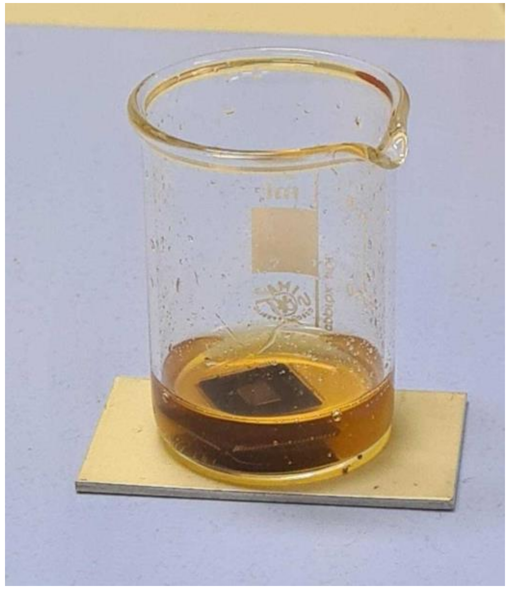
a) Physical samples

b) Anonymized GDS-II

MILLING / ETCHING / IMAGING



a) X-Prep milling device



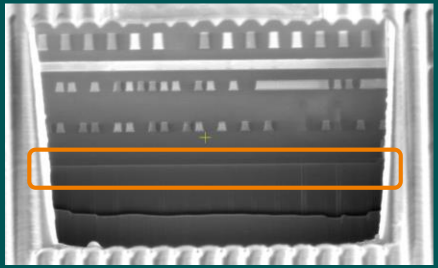
b) Choline Hydroxide Etching

(No Picture available)

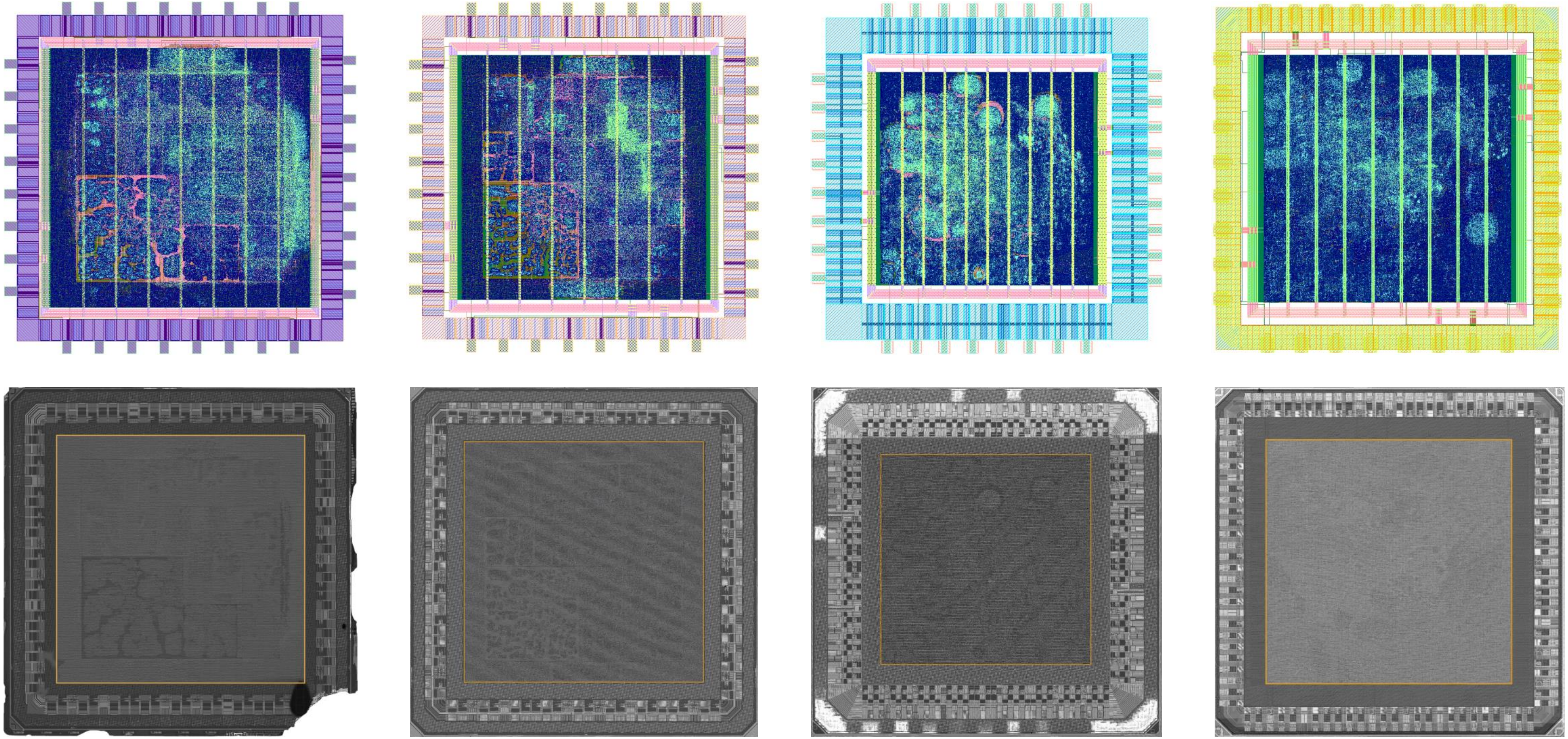
c) FIB / SEM

Cross-section Side View

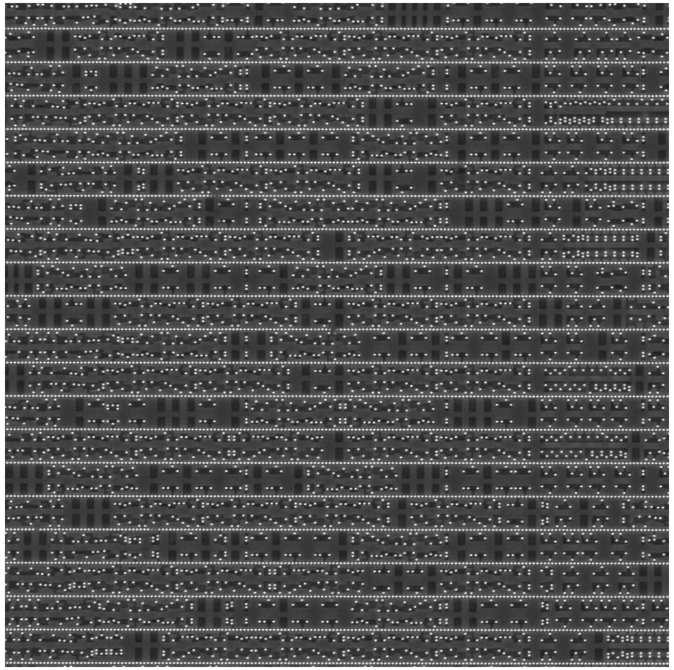
- Cell Layout: Bottommost Layer
- Removing Silicon from the bottom
- Imaging from the bottom



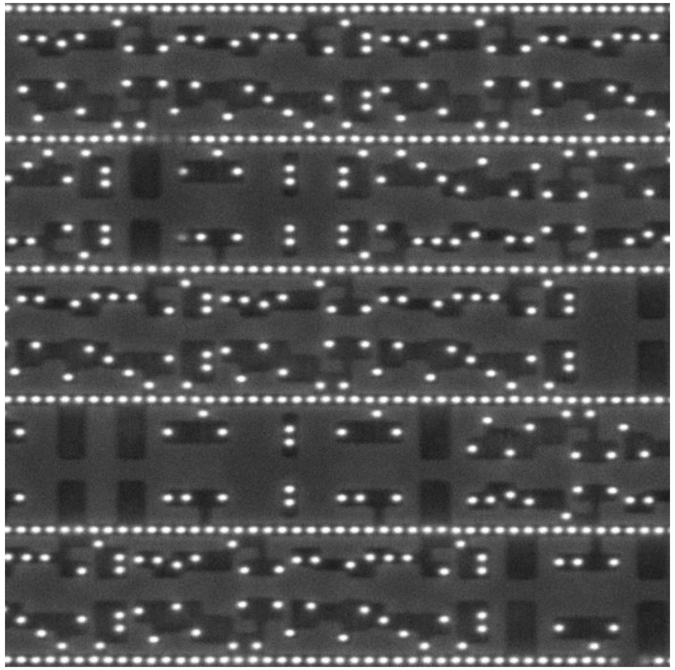
LAYOUT VS. SEM BACKSIDE IMAGE



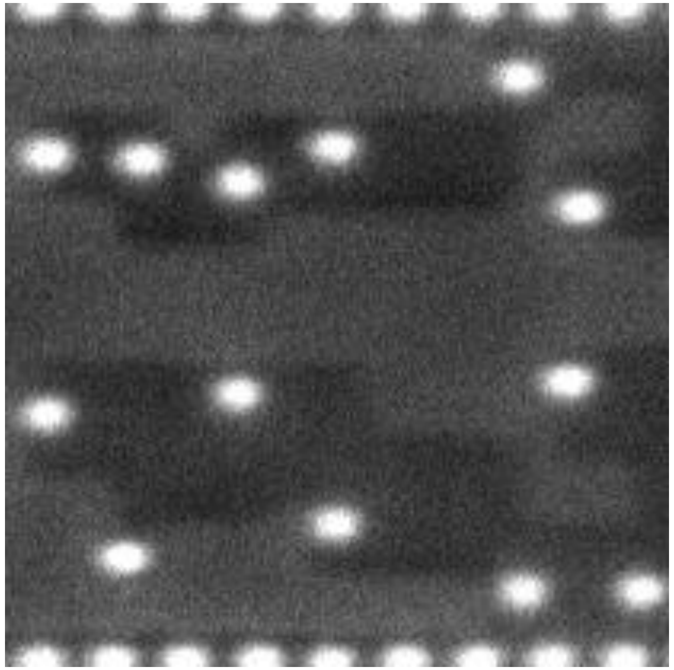
90NM CHIP SEM-IMAGES



a) Full Tile

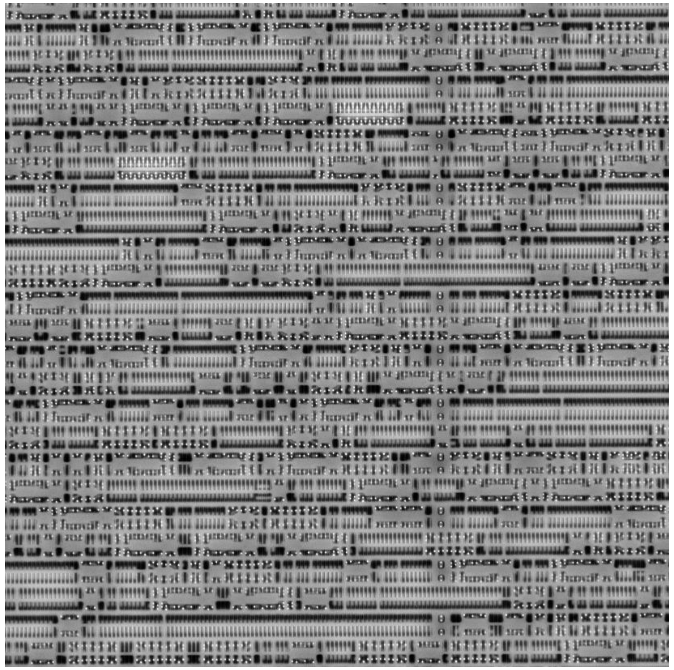


b) Zoom 1

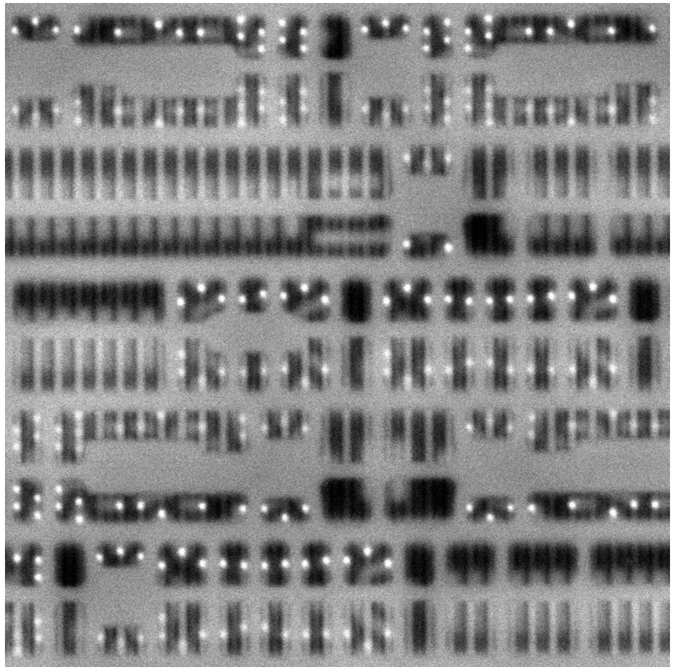


c) Zoom 2

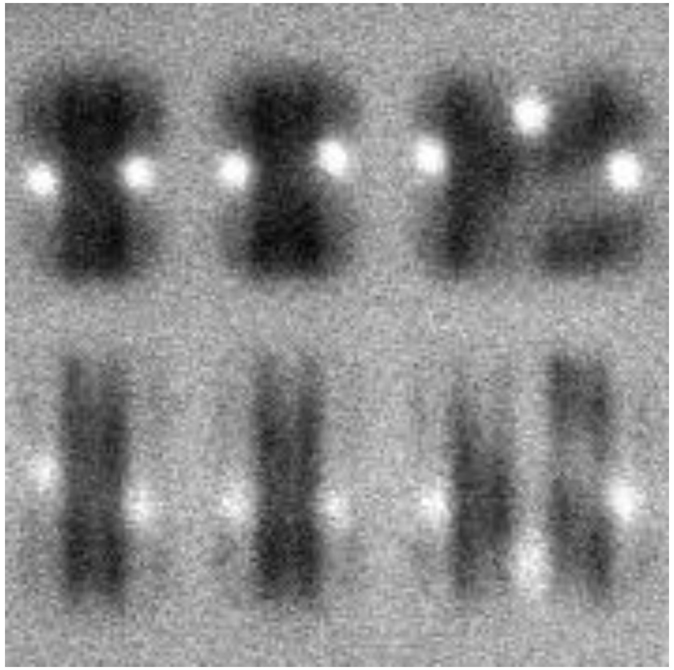
28NM CHIP SEM-IMAGES



a) Full Tile

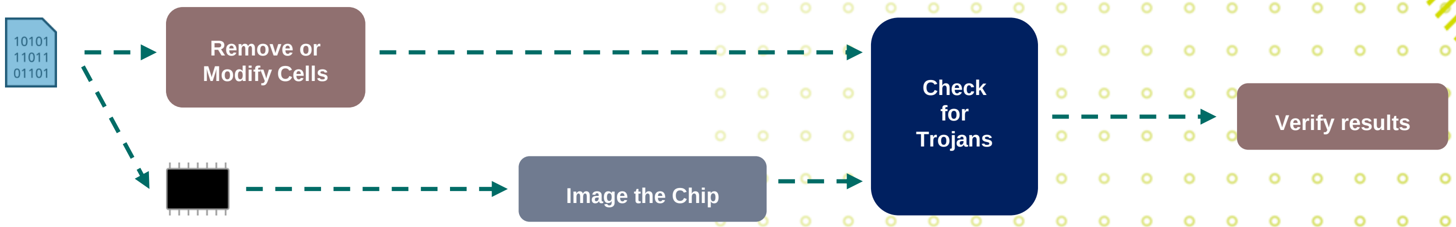


b) Zoom 1



c) Zoom 2

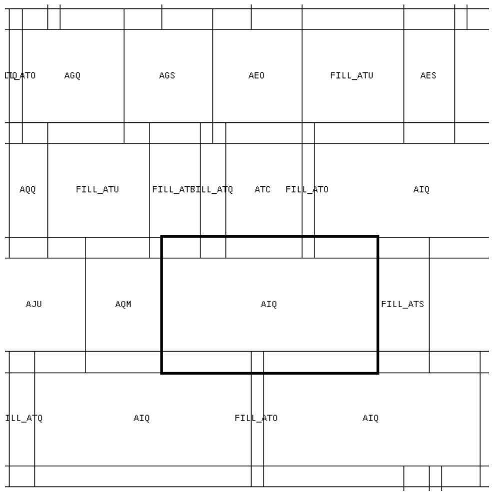
BLUE TEAM: CHECK FOR TROJANS

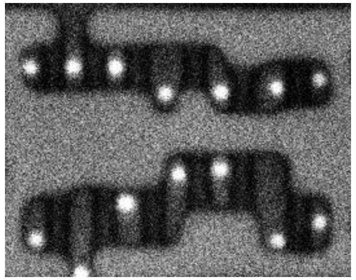


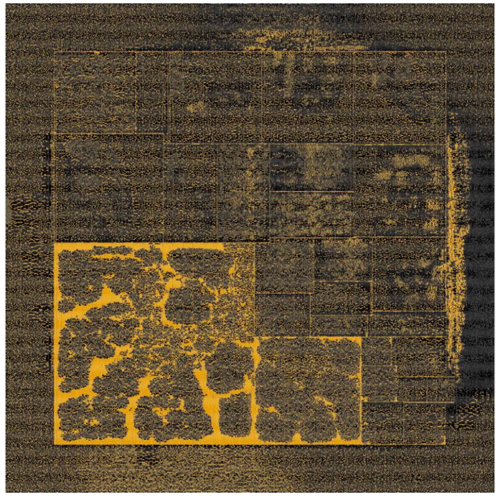
FIRST STEPS

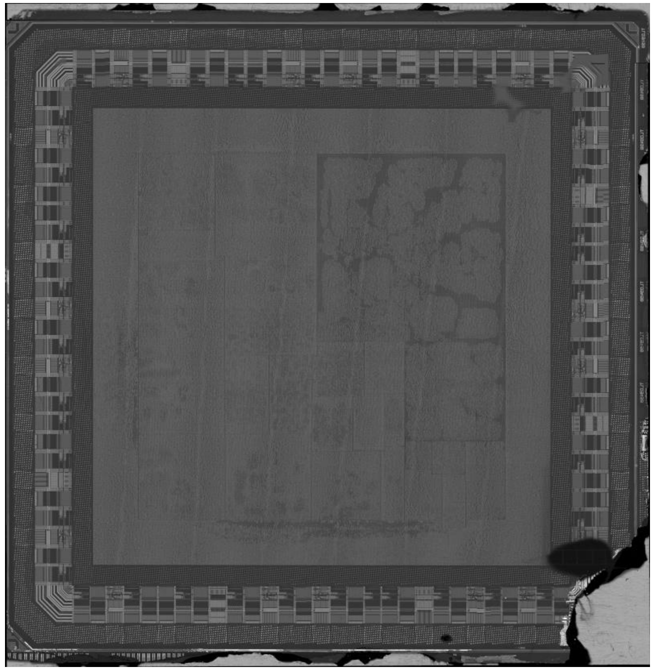
Towards Cell Comparison

- For each cell from the design file
- Cut matching one out from the microscope images





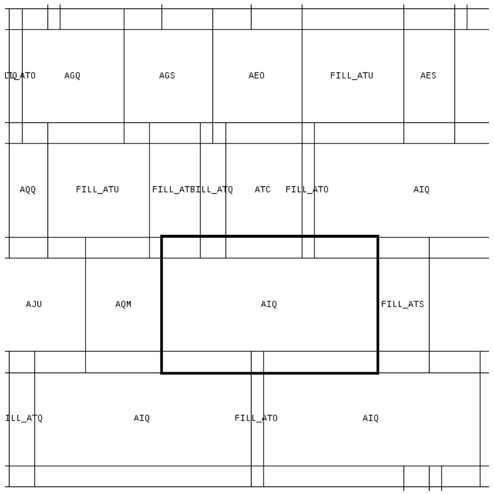


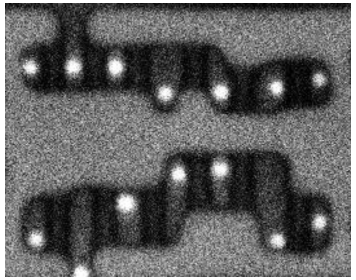


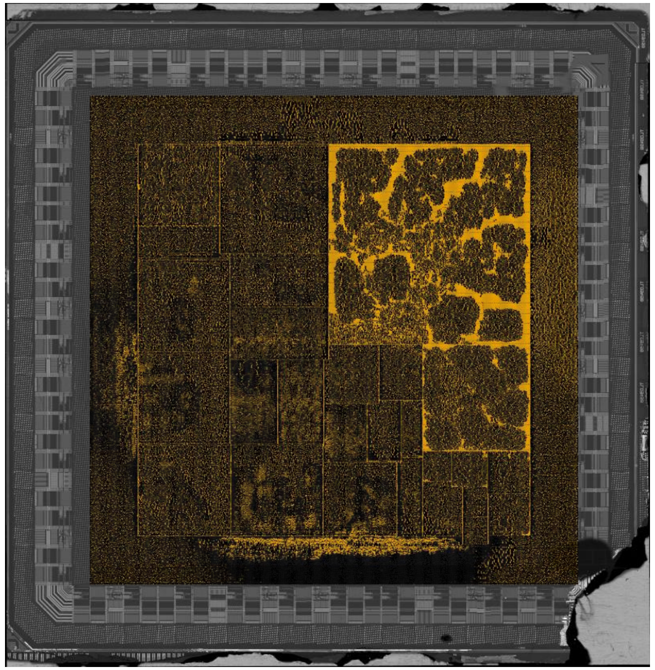
FIRST STEPS

Towards Cell Comparison

- For each cell from the design file
- Cut matching one out from the microscope images



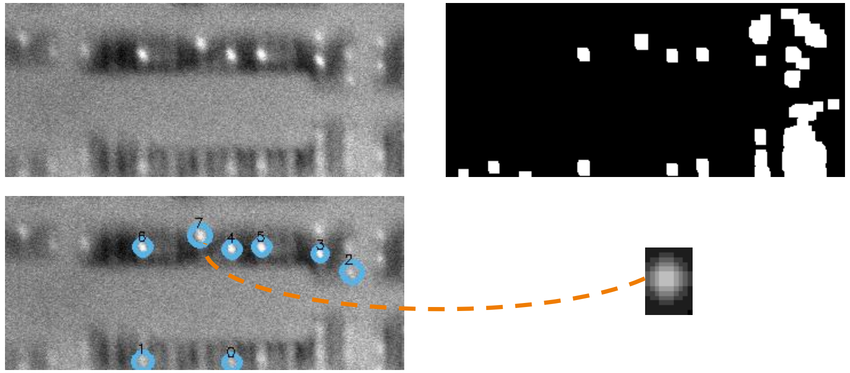


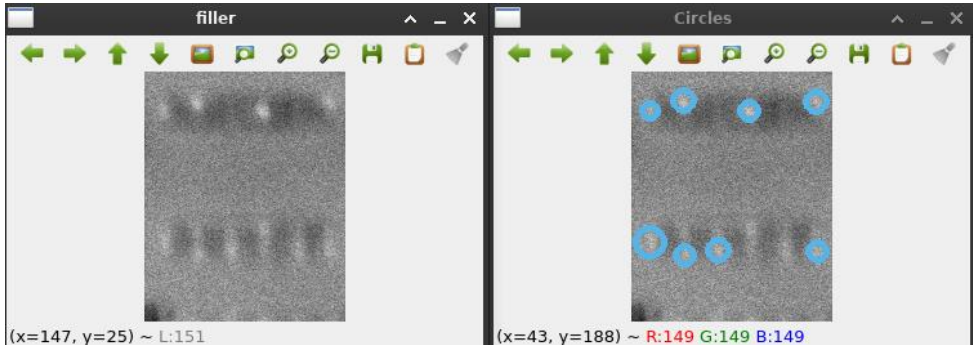


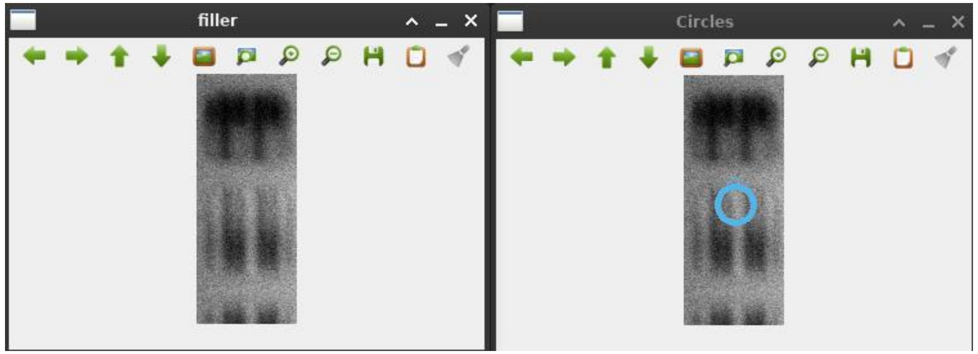
FINDING LOGIC CELLS WHERE FILLER CELLS ARE EXPECTED

Cells contain vias, let’s detect them

- Approach:
  - Suppress noise, threshold, find spots of defined size
  - Verify that they have enough variance (=contrast)
  - Also build a gradient and correlate (corr > x = via)





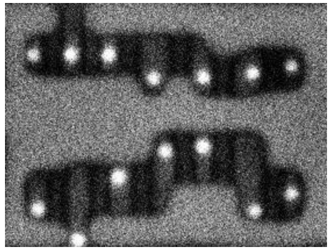


In the end, depends on image quality and parameters

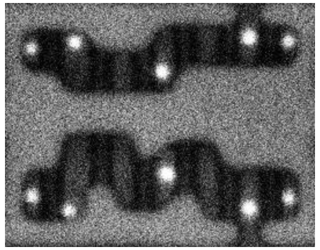
→ some false positives

FINDING CELL REPLACEMENTS

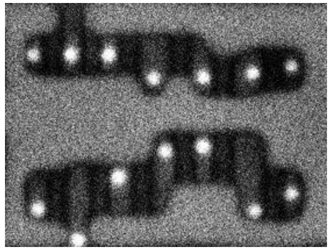
- Q: “Is the cell in question the one it is labeled, or was it replaced by another cell?” (e.g., AND → OR)



Golden Model / Template



Other Cell labeled same

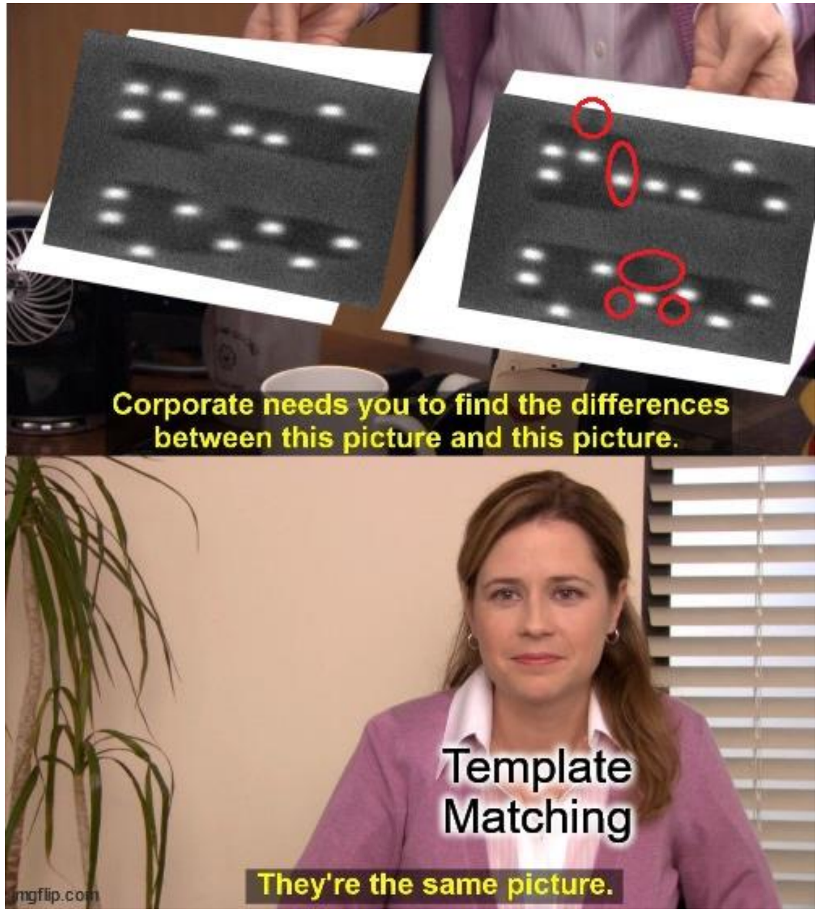


Other Cell labeled same

→ Template Matching

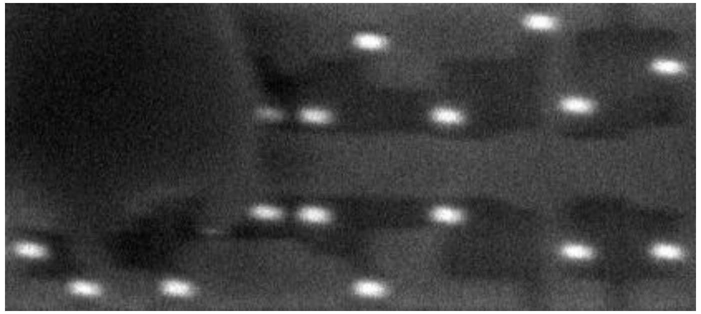
- Use a golden reference model to compare each cell of the same type (= label) against
- If different, count as candidate for modification

TEMPLATE MATCHING VS. SIMILAR CELLS

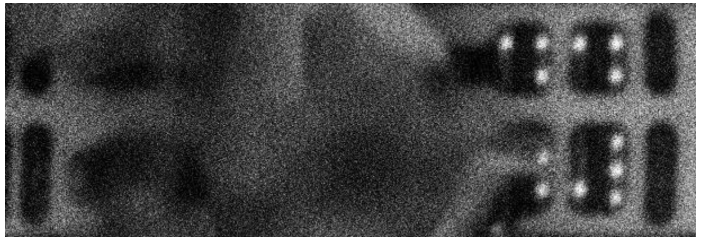


EXEMPLARY FALSE POSITIVES CAUSED BY:

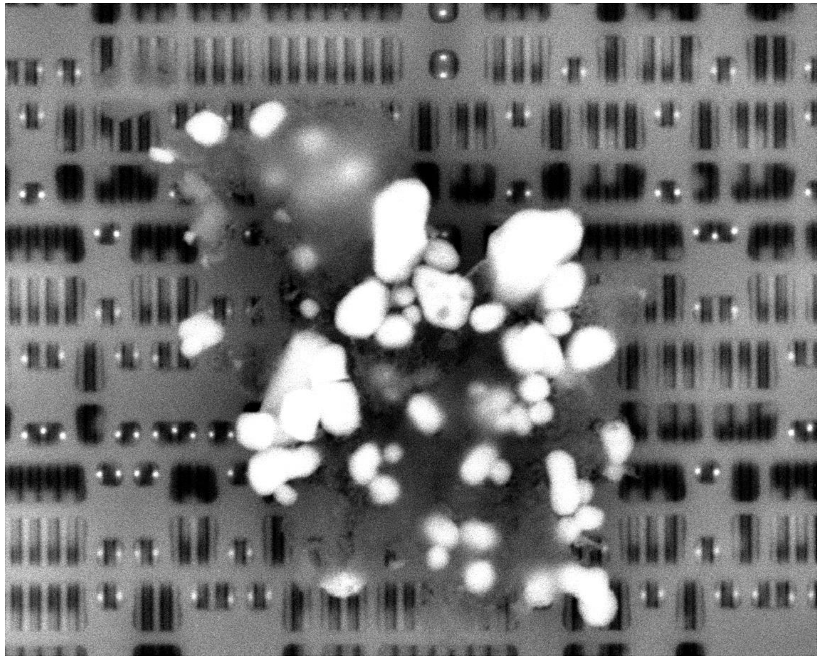
Debris / Dust



a) 90nm example



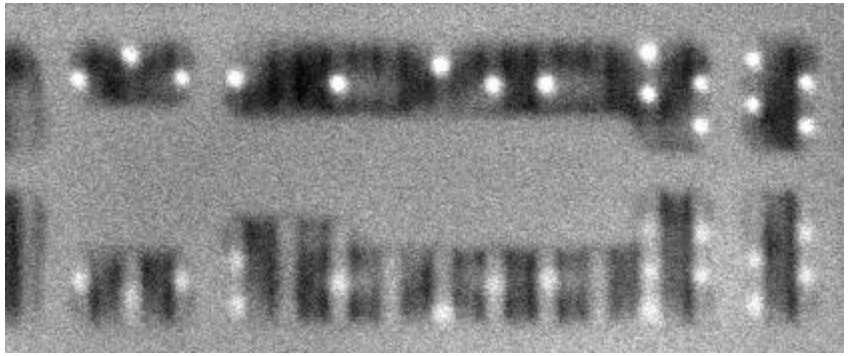
b) 40nm example



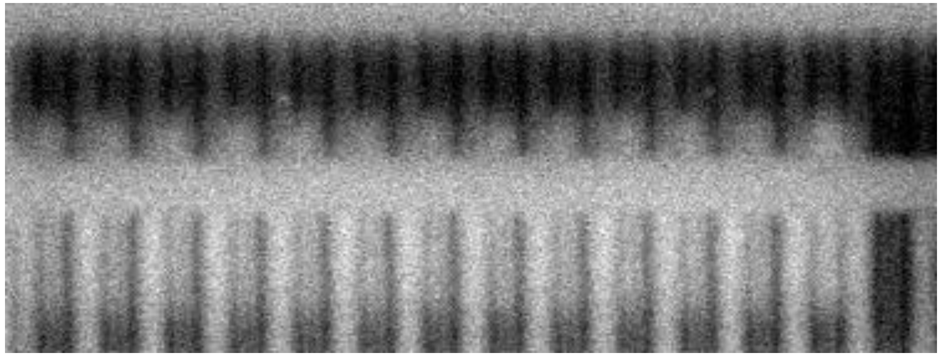
c) 28nm example

EXEMPLARY FALSE POSITIVES CAUSED BY:

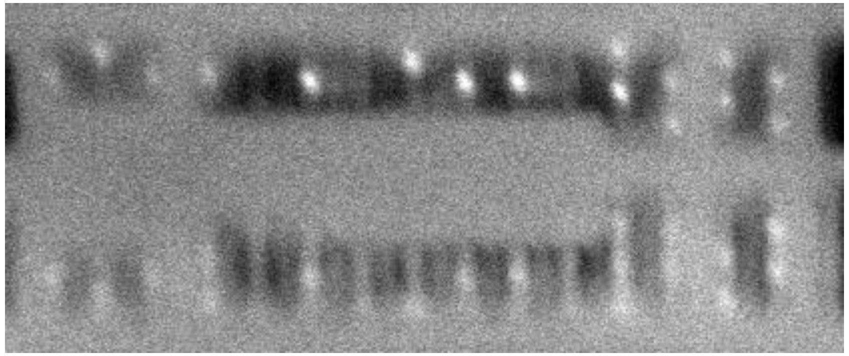
Contrast (& Blur)



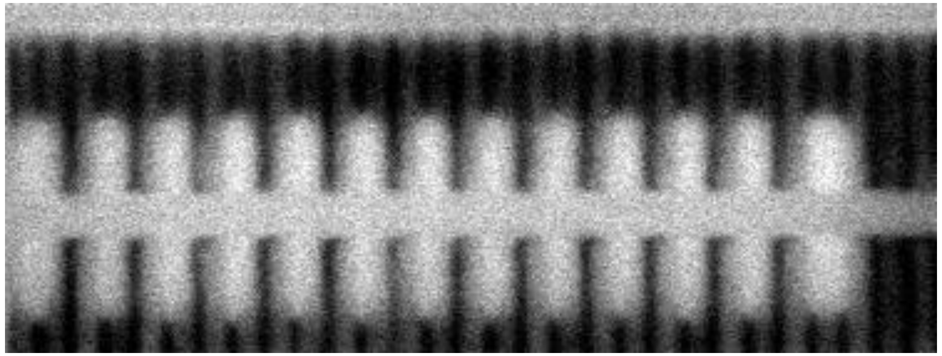
a) template



a) template

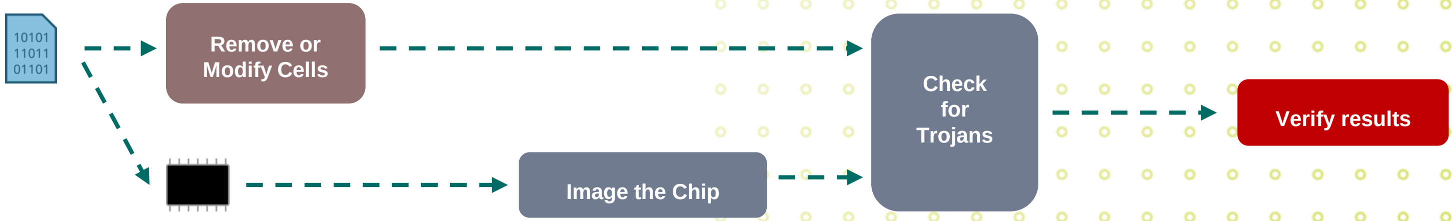


b) instance

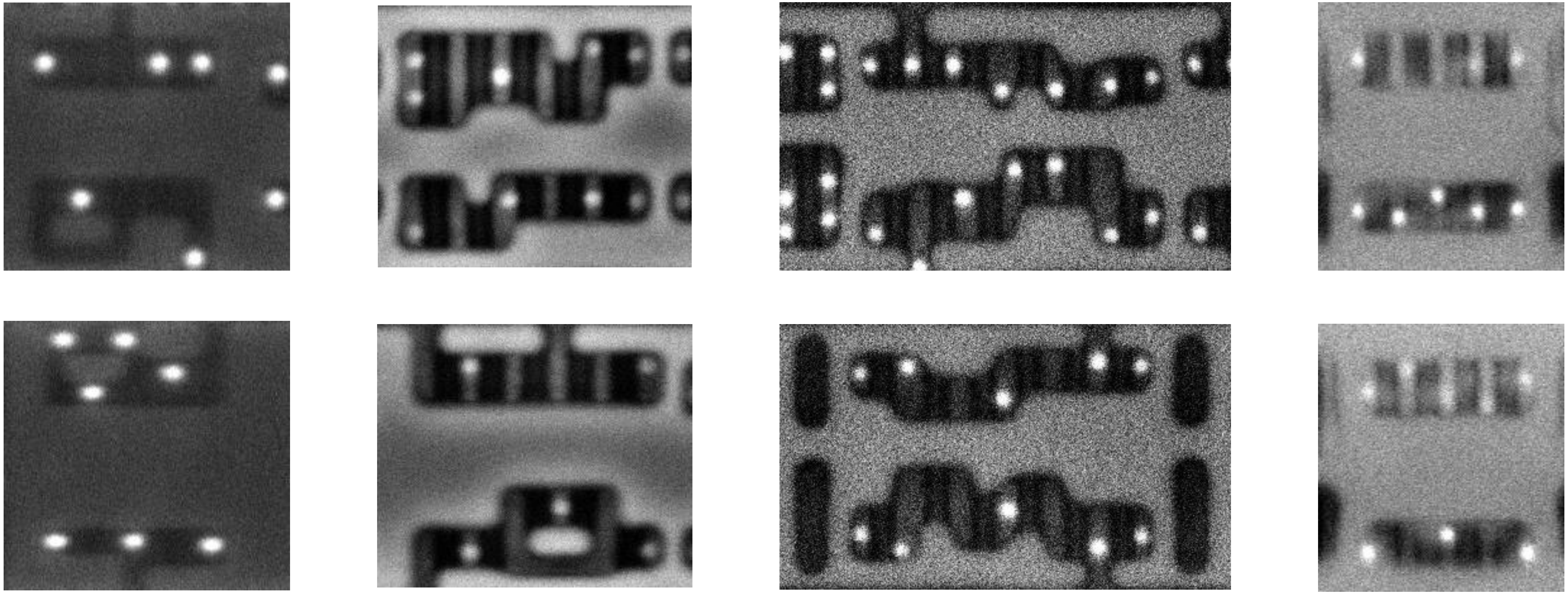


b) instance

RED TEAM: VERIFY RESULTS



EXEMPLARY TRUE POSITIVES

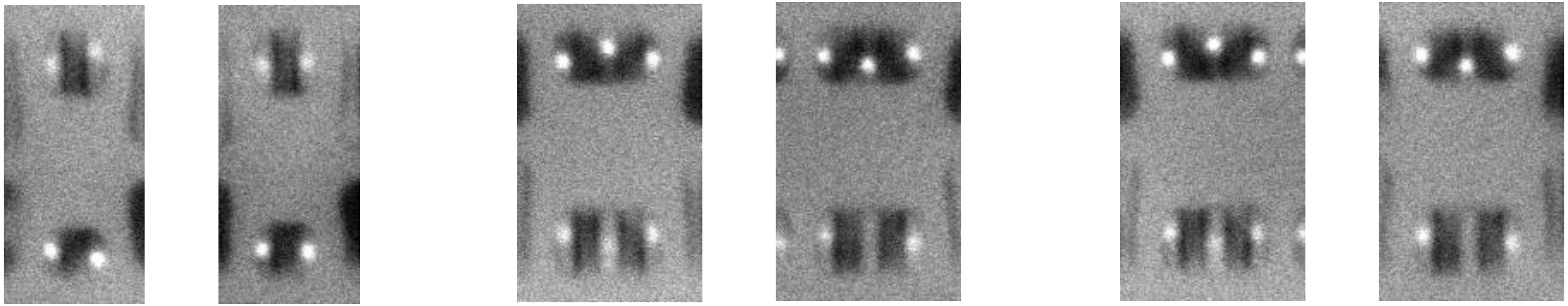


a) 90nm b) 65nm c) 40nm d) 28nm

RESULT OF THE STANDARD CELL REPLACEMENT DETECTION

	90 nm	65 nm	40 nm	28 nm
Filler Cell Replacements	4 ✓	4 ✓	4 ✓	4 ✓
False Positives	0	0	4	17
Functional Replacements	6 ✓	6 ✓	6 ✓	3 ✗
False Positives	136	6	11	343

FALSE NEGATIVES



- Finding these difference is not feasible with our current algorithms
- Can you do better?
  - Approach to get images with less noise etc. from a SEM?
  - Build better algorithms (involving ML?) for low quality images

CONCLUSION

- With sufficient image quality, cell replacements can be found with classical image algorithms
- Even minimal trojans can be found
- Destructive process, probably sufficient to check few samples
- The number of false positive results is considerably low

- We published chip images, (reduced) design files and programs for further research in this area:
  - ↘ *Paper:* *https://eprint.iacr.org/2022/1720*
  - ↘ *Images / Design Files:* *https://doi.org/10.17617/3.396Q7I*
  - ↘ *Code:* *https://github.com/emsec/ChipSuite*
- Limited chips available for further analyses

THANKS FOR YOUR ATTENTION

If you got any questions, feel free to reach me:

Max Planck Institute for Security and Privacy

Universitätsstr. 140, 44789 Bochum

Phone: +49 (0)234 90498-106

Email: endres.puschner@mpi-sp.org
Internet: https://www.mpi-sp.org

LINK TO THE PAPER

https://eprint.iacr.org/2022/1720

LINK TO THE DATA

https://doi.org/10.17617/3.396Q7I