# ADVANCED IC REVERSE ENGINEERING TECHNIQUES: IN DEPTH ANALYSIS OF A MODERN SMART CARD

Olivier THOMAS <olivier@texplained.com>

Blackhat USA 2015

# About Texplained

## Texplained [Technology Explained]

refers to  the skill of making sense out of any IC in a black box situation

## Invasive attacks

Invasive attacks are left out of evaluation and  certification mainly because of the extensive resources needed

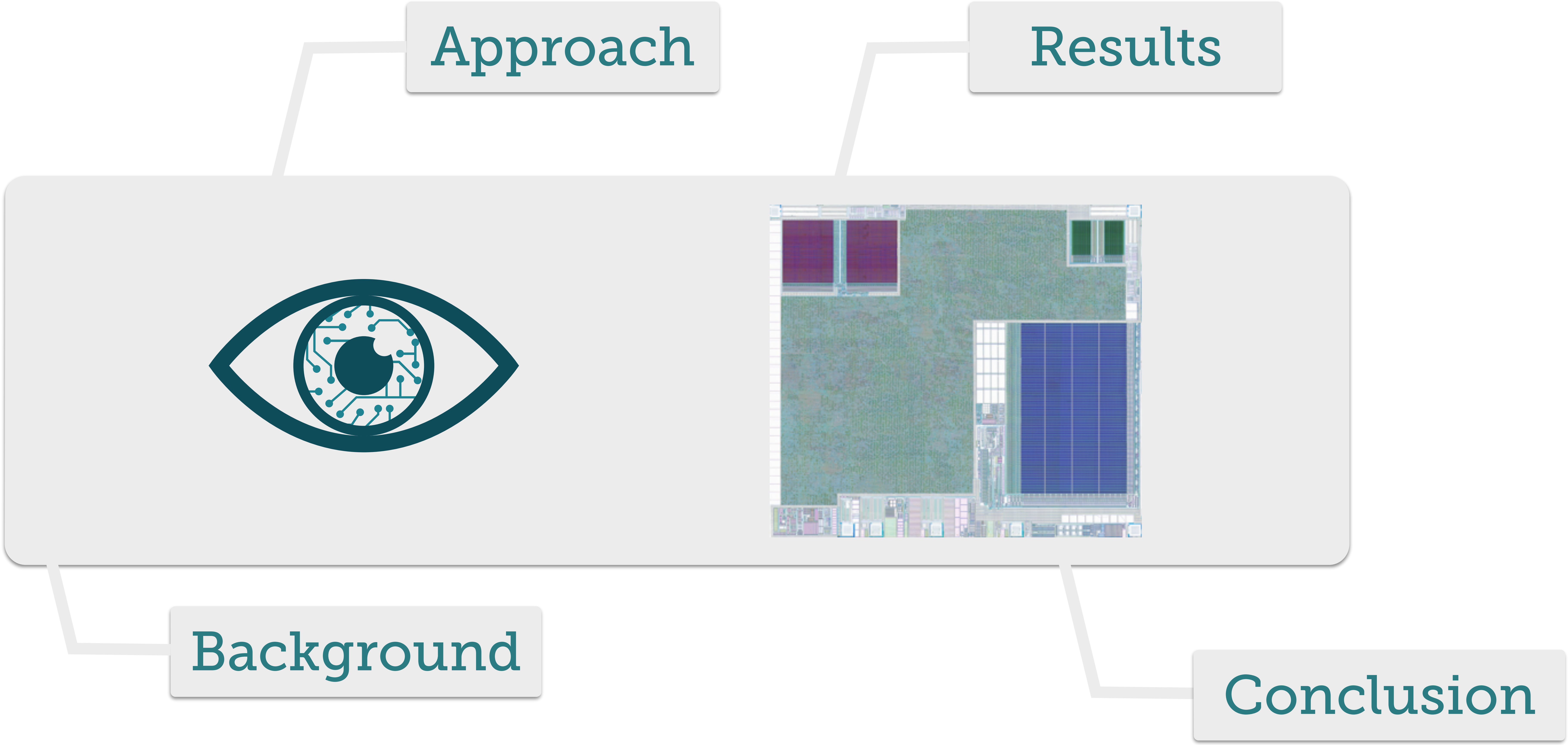
Whereas Invasive attacks are a major threat as:

- Piracy and counterfeiting have merged
- Hackers groups are getting professional

Texplained focuses on performing invasive analysis using the technologies developed in house to perform complicated analysis in a short amount of time

Expertise in Texplained comes from 10 years of active R&D experience for an independent security research laboratory focused on demanding pay-tv security

# Overview



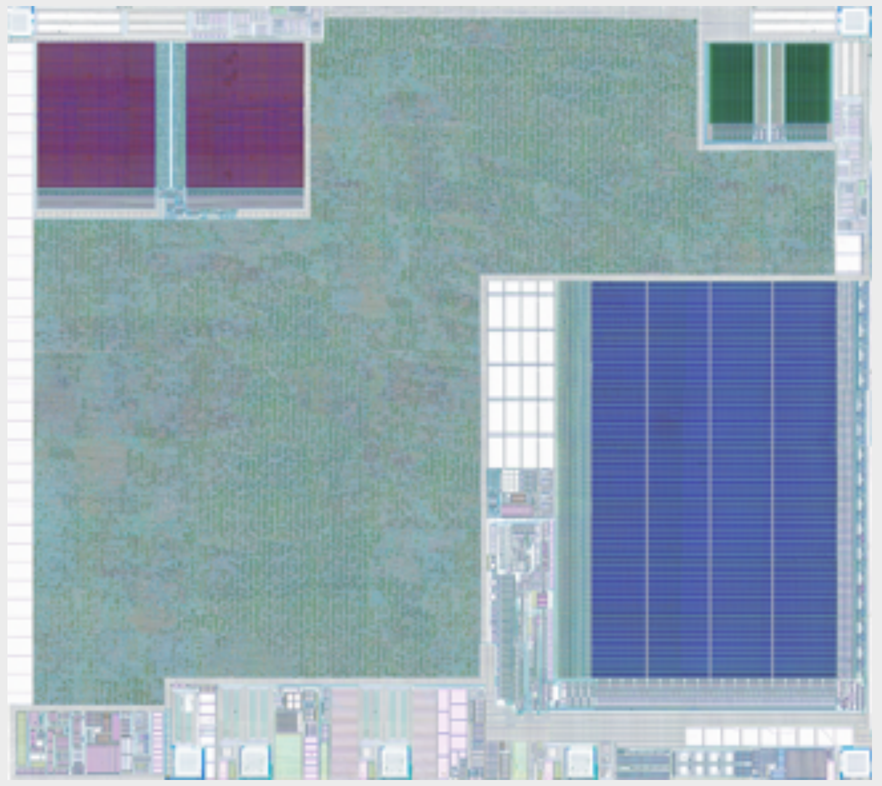
Approach

Results

Background

Conclusion

# Overview



Background

# Background

## Secure Microcontrollers

- This talk will focus on secure microcontrollers.
- A secure microcontroller is an Integrated Circuit (IC) with an integrated CPU, program memory and storage for sensitive data.
- Secure microcontrollers are available in different form-factors:
    - Smartcards, biometric passports and ID cards
    - SMD packages for TPMs, uSD, UMMC
- Members of a particular product family will share device characteristics.

# Background

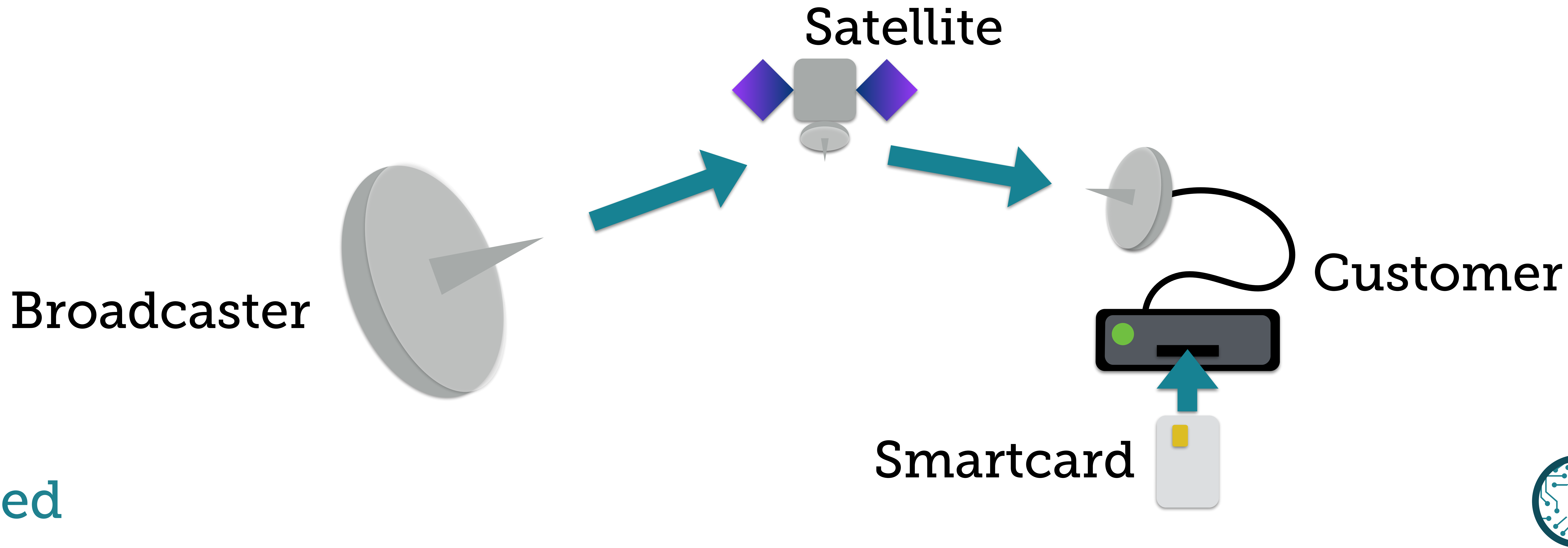
## Evaluation

- When it comes to invasive attacks, one can argue that the attack is time and ressource consuming.
- BUT equipment can be rented and / or service labs can provide support
- There is no clearly defined process to study one IC in a reasonable time
- Invasive Attacks are under evaluated

# Background

## Pay Tv

- Pay Tv has been the first market to suffer from heavy piracy

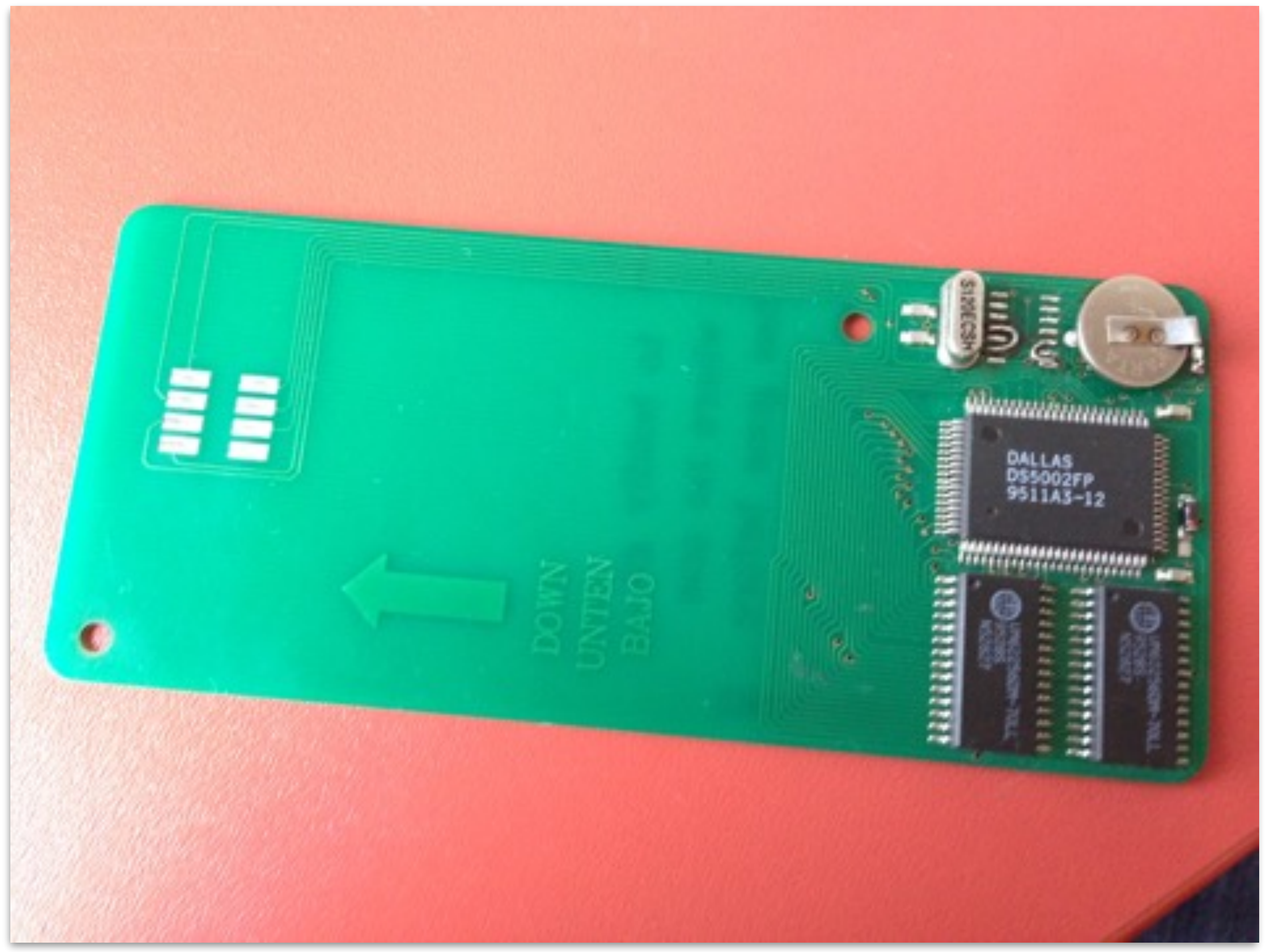


# Background

## Pay Tv

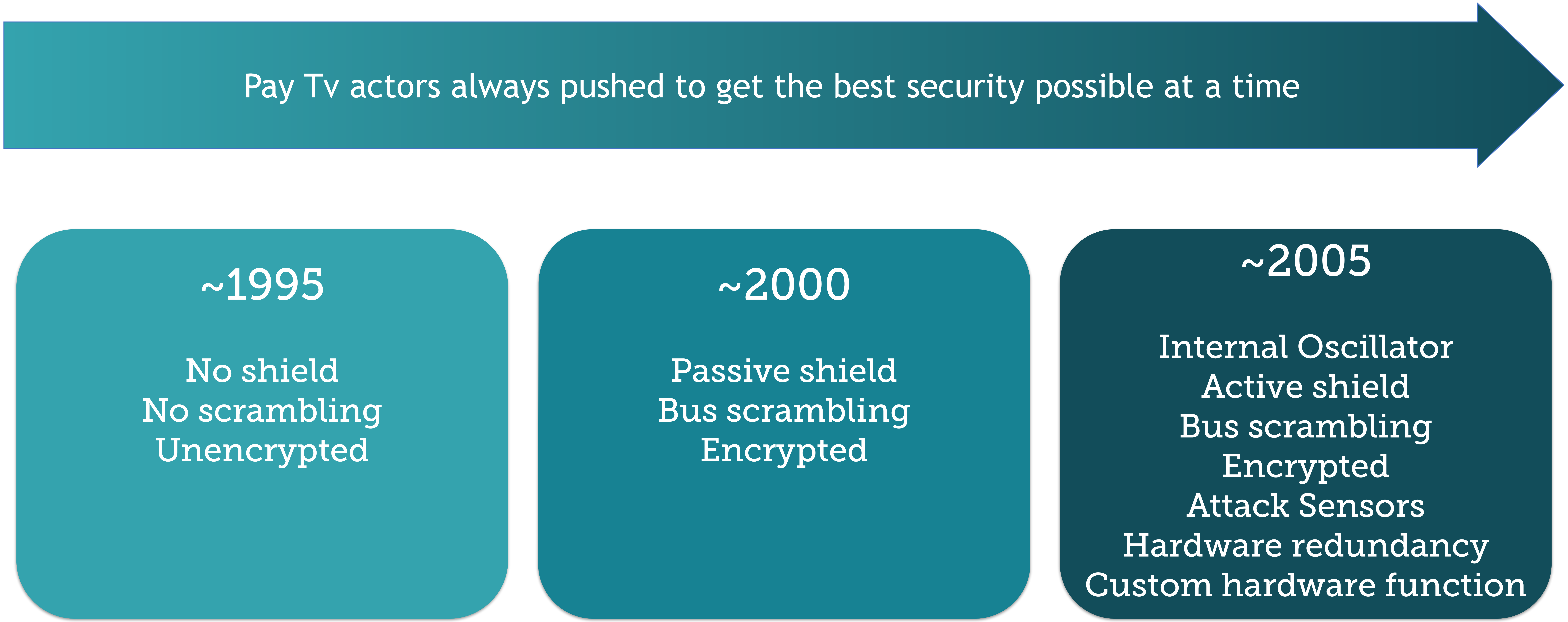
### The problem

A clone of a PayTV subscriber card will have the same level of access as the genuine subscriber card. Pirates can buy a single subscription with access to all the paid content and then produce copies of this card.



Pirate Card ca. 1995

# Evolution



Pay Tv actors always pushed to get the best security possible at a time

~1995

No shield
No scrambling
Unencrypted

~2000

Passive shield
Bus scrambling
Encrypted

~2005

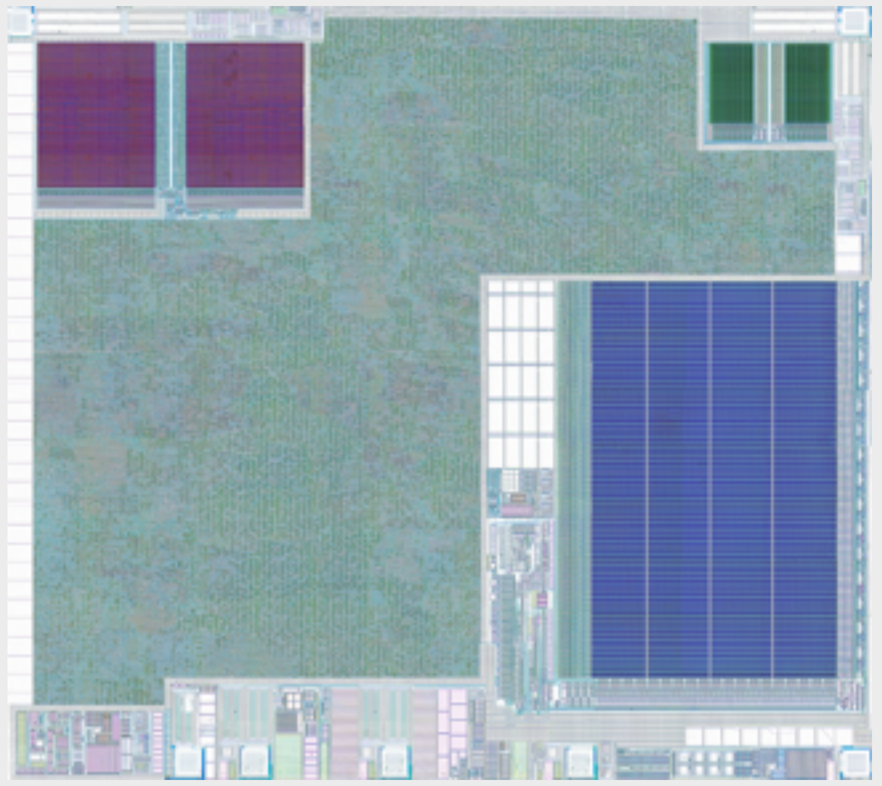
Internal Oscillator
Active shield
Bus scrambling
Encrypted
Attack Sensors
Hardware redundancy
Custom hardware function

# Threat globalisation

- Piracy is not the only threat anymore
- Supply chain security is of concern for fabless manufacturers (backdoors)
- IP theft could be a critical issue
- Counterfeiting has become a bigger market
- Mass selling products are the new targets
  - Consumables (Ink cartridges for printers, ...)
  - Accessories (game console controllers, ...)
- Internet Of Things will create a global security need

# Overview

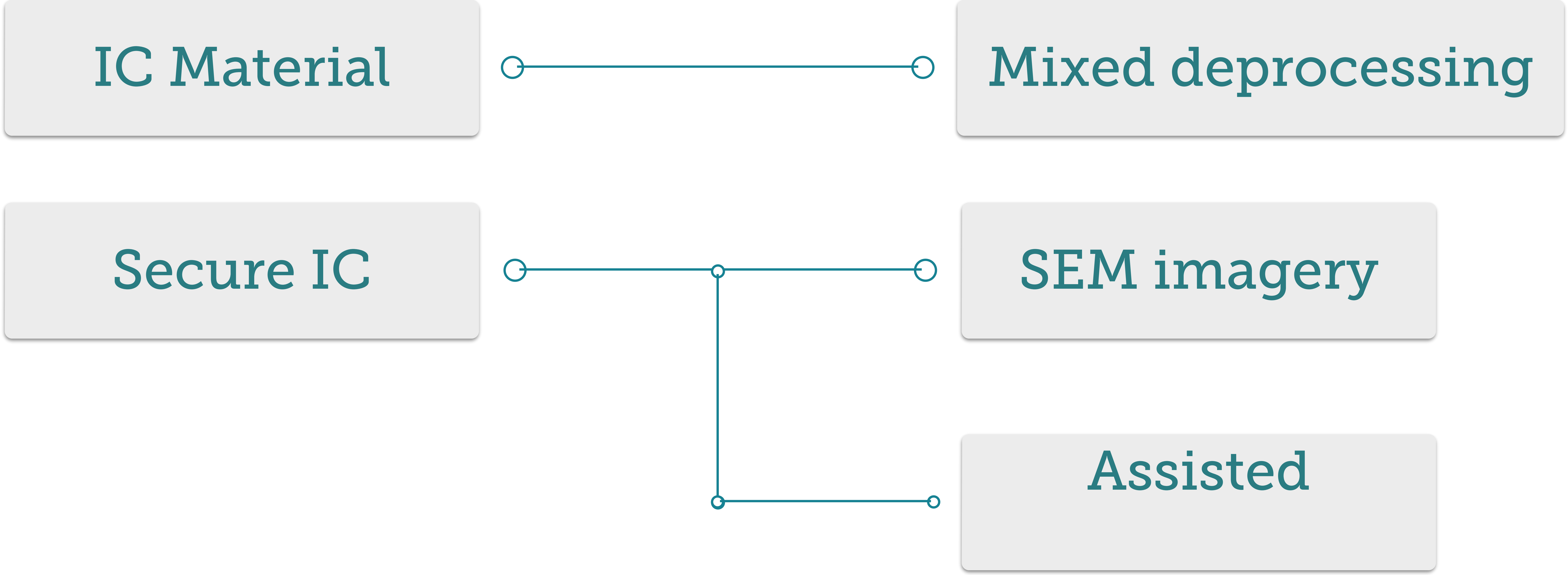
Approach



# Approach

- Research Project about new analysis methods - work in progress
- Time and ressource limited project (one person - one month).
- The Target : State Of The Art Secure Smart Card
    - shield (mesh)
    - memory encryption
    - internal oscillator…
- Analysis methods
    - professional deprocessing
    - high resolution imagery (Scanning Electron Microscope)
    - Labless analysis through custom tools

# Process Choices



IC Material

Mixed deprocessing

Secure IC

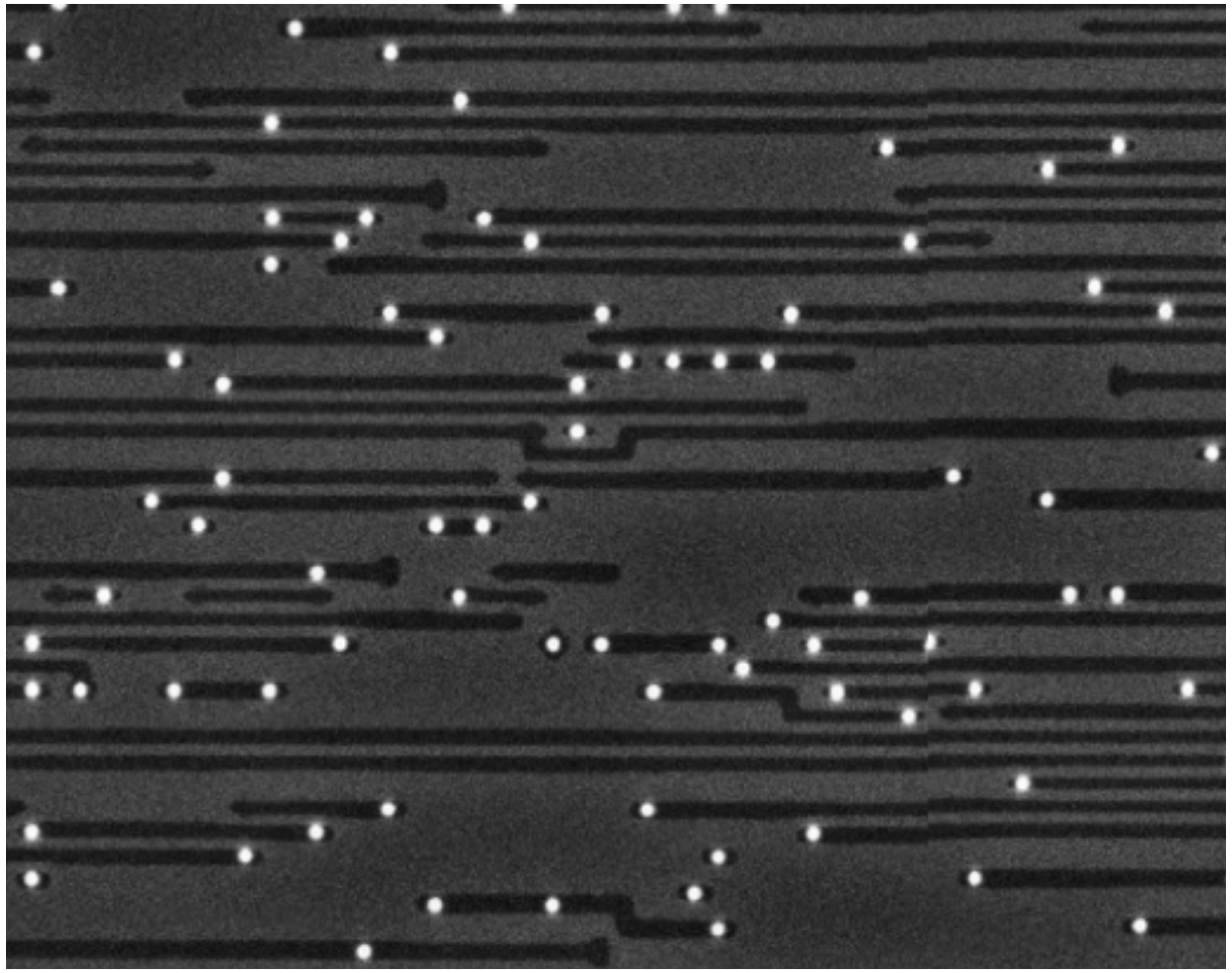
SEM imagery

Assisted

# DeProcessing

Card Material → Mixed deprocessing

- Chip is Aluminium based
- This means :
  - Lines are made of Aluminium
  - Vias are made of Tungsten
- Therefore, it is possible to :
  - remove lines
  - keep the vias



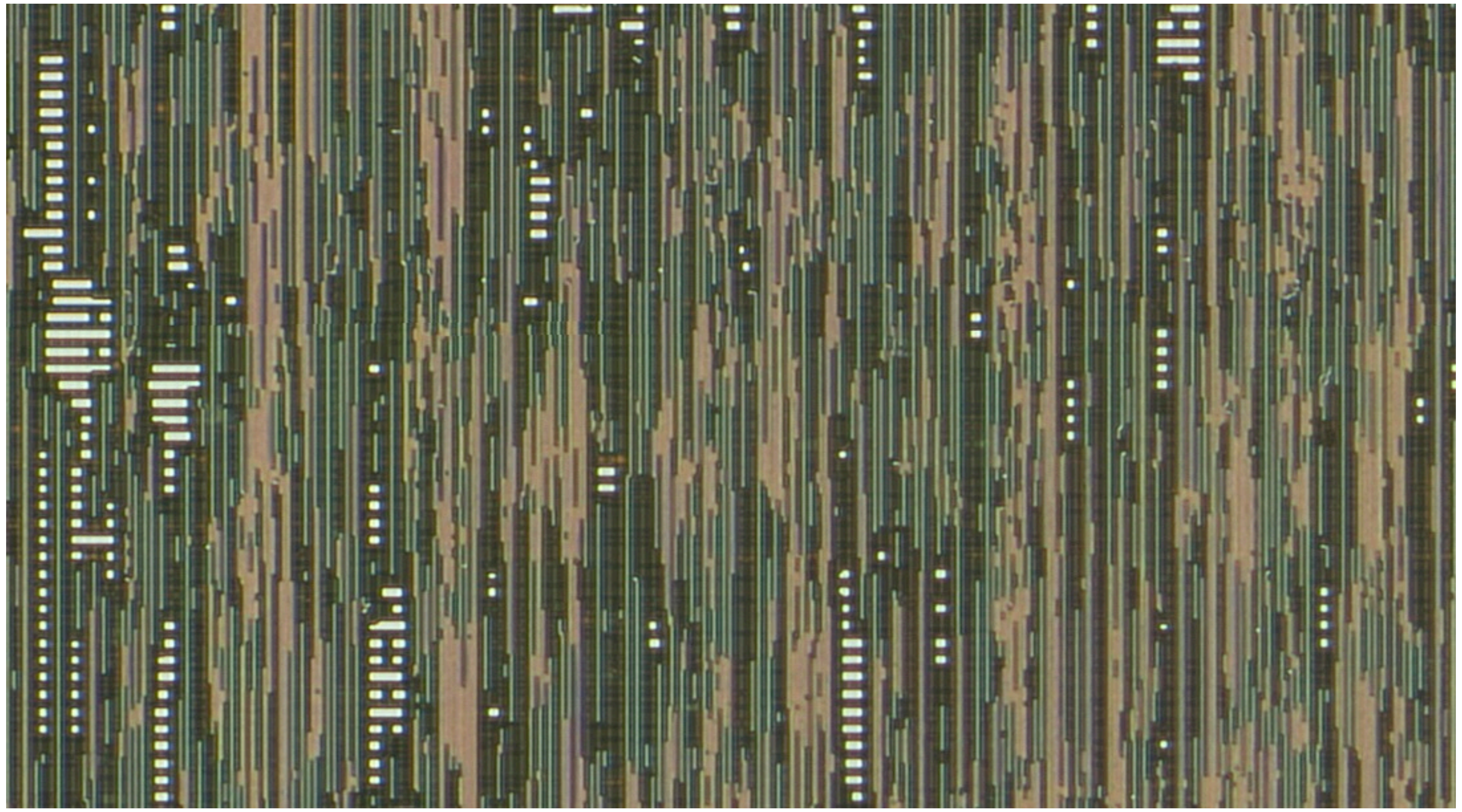
Texplained

# Imagery

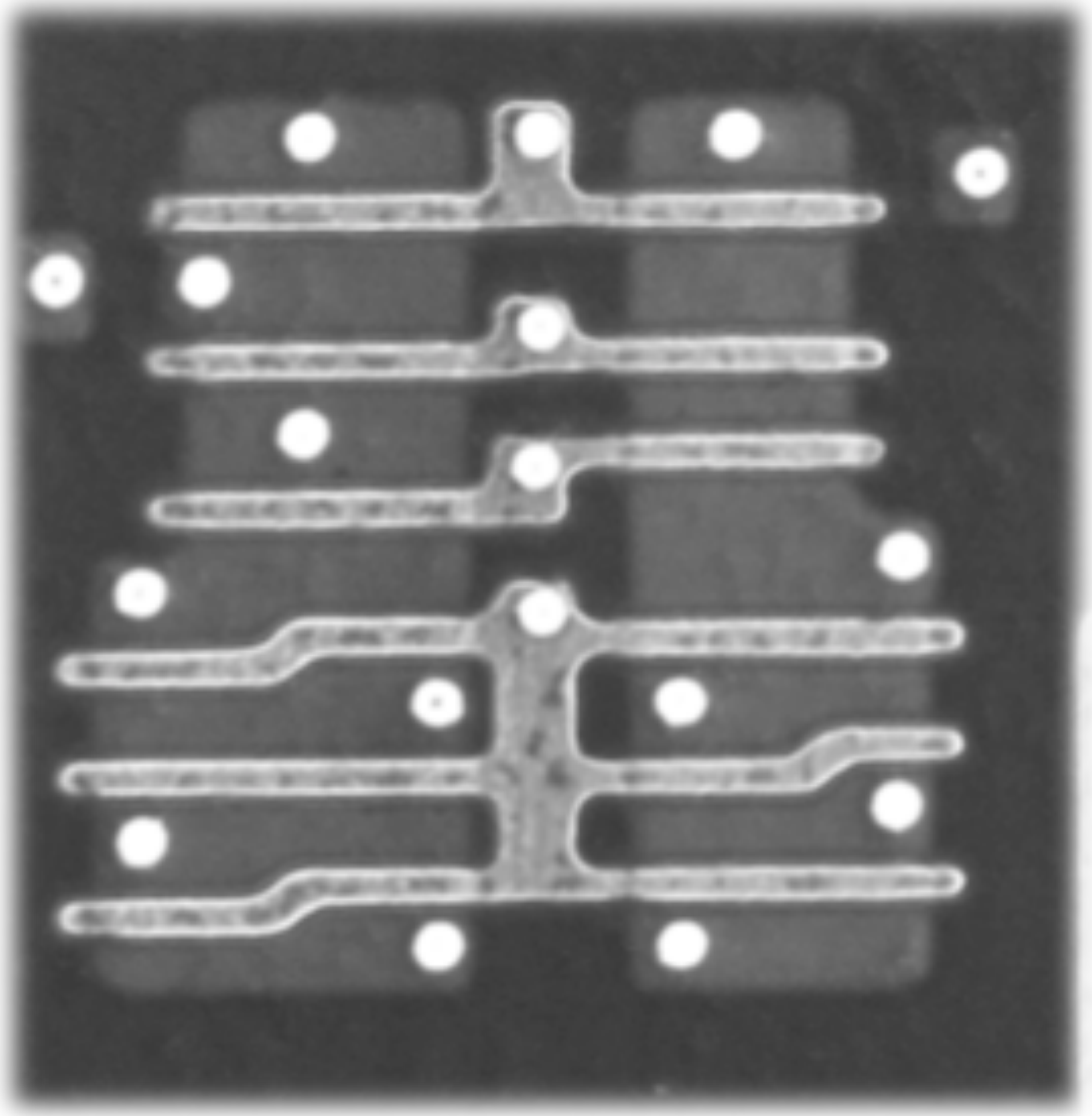
Secure IC

SEM imagery

- Optical pictures are not usable
- SEM brings high resolution



*Optical Picture*



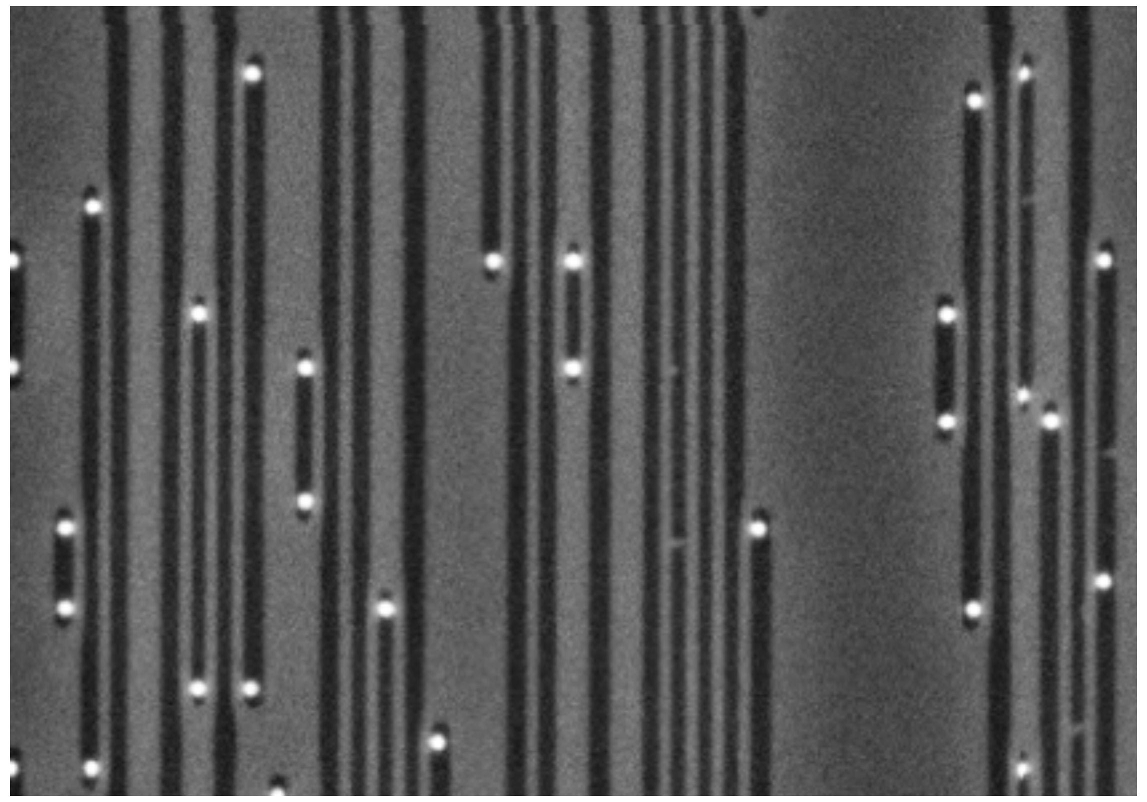
*SEM Picture*

# Imagery

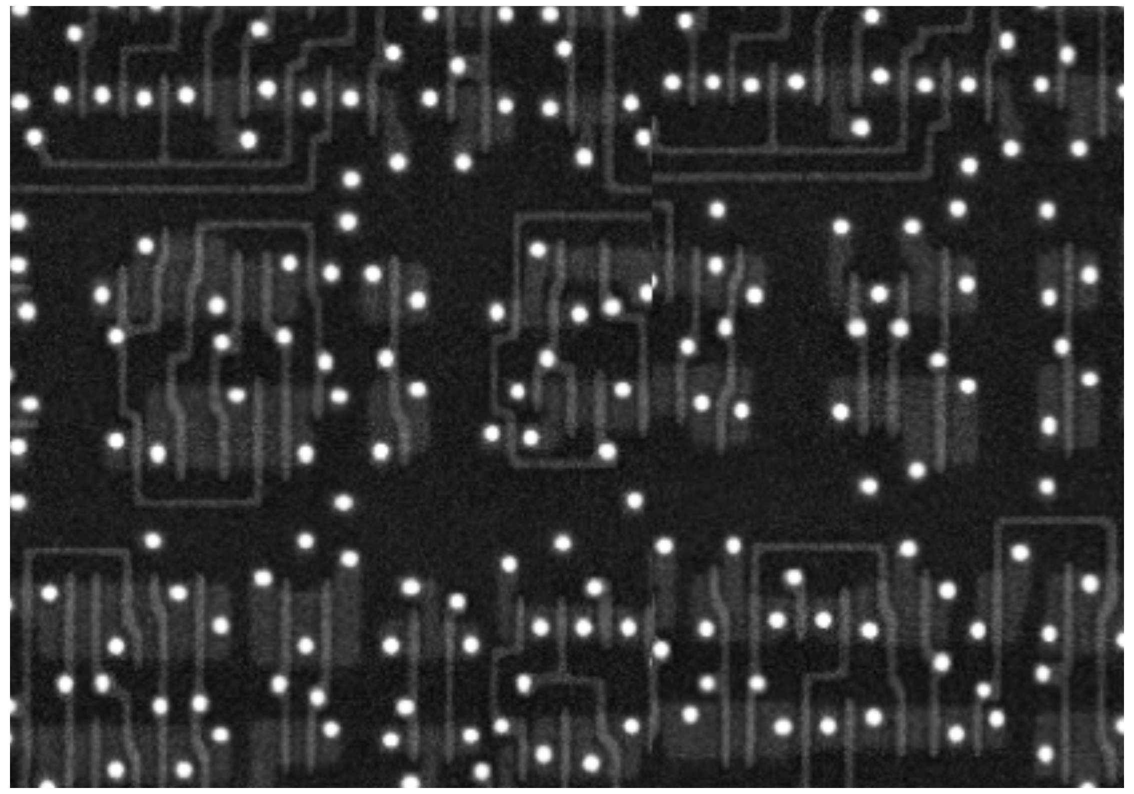
Secure IC

SEM imagery

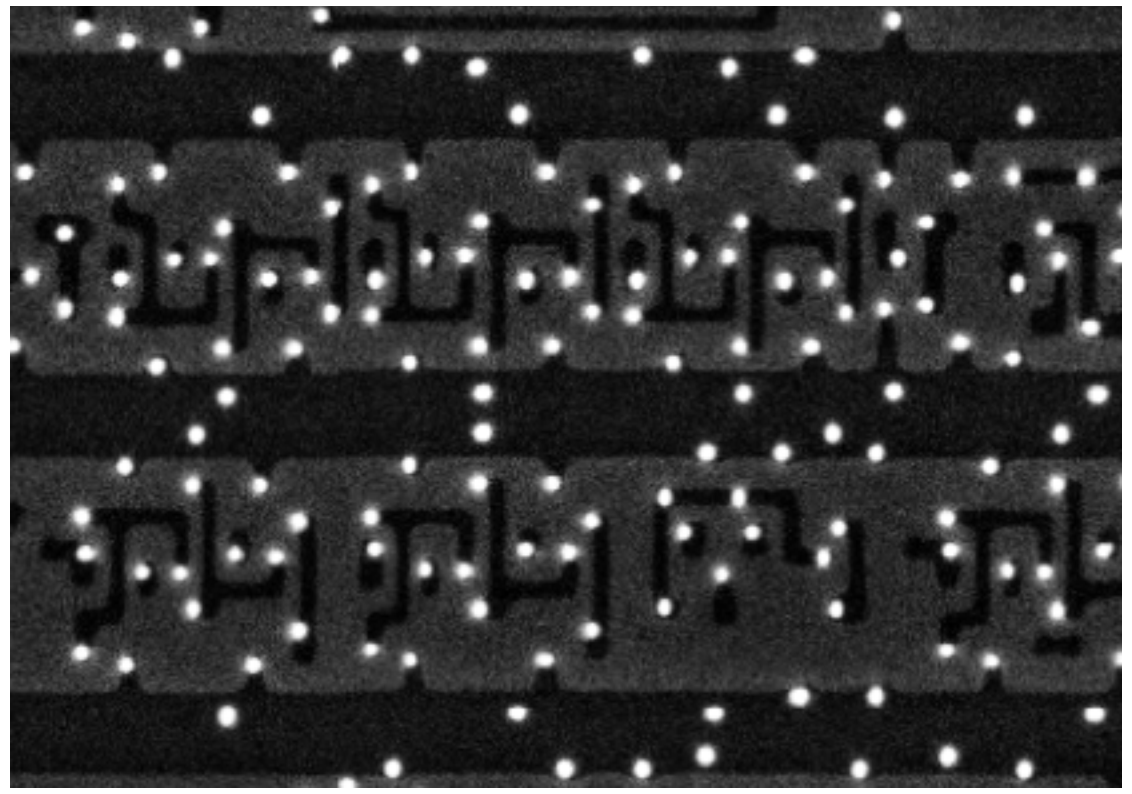
- 5 layers have been imaged (4 interconnect layers + active layer
- 1500 pictures per layer



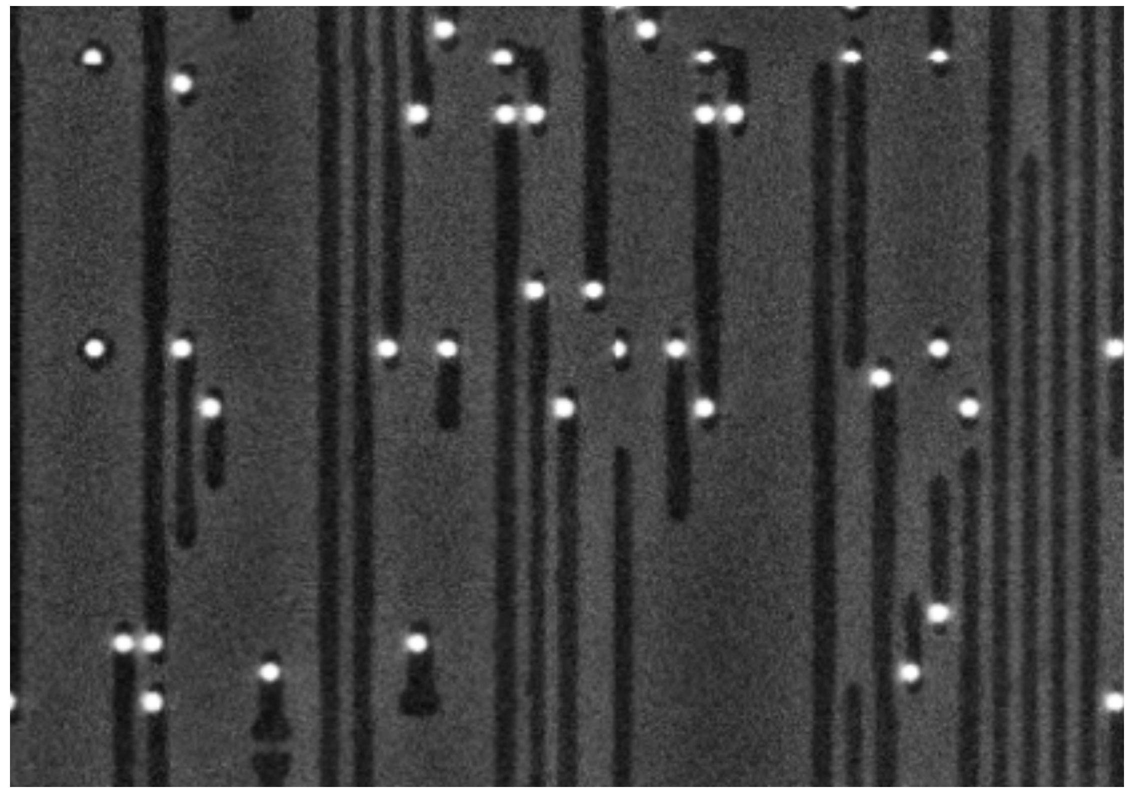
*Metal 4*



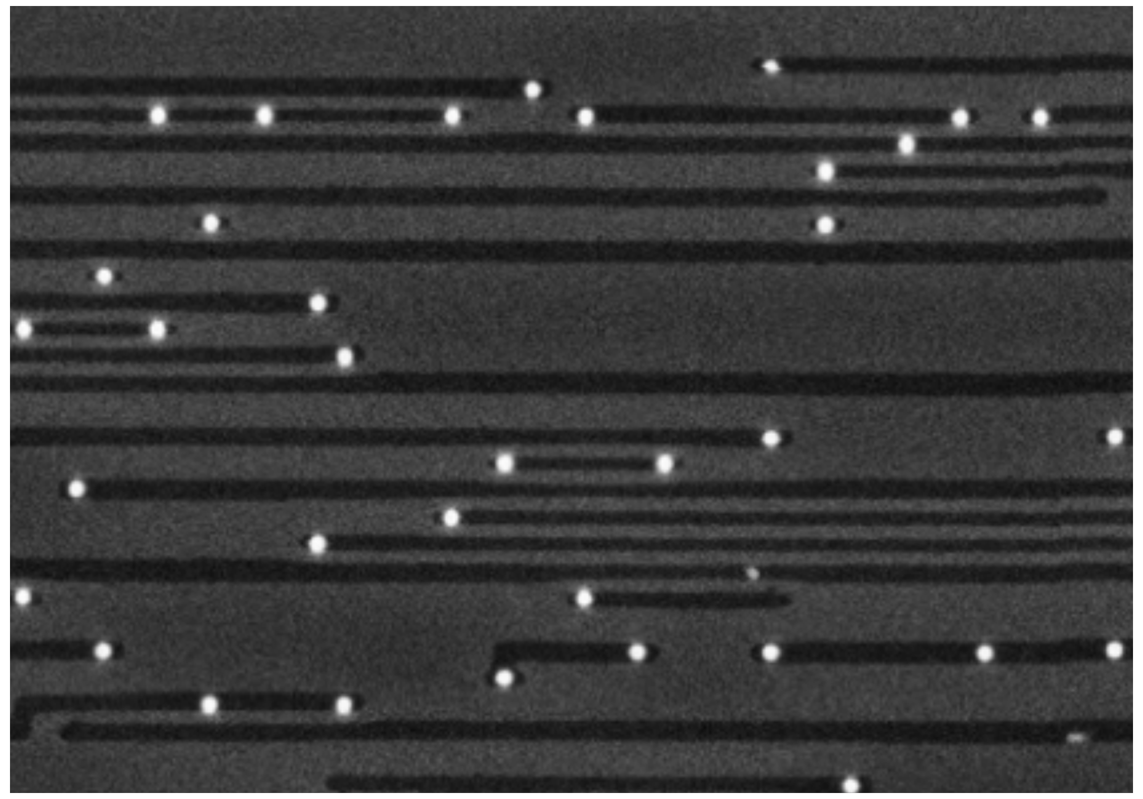
*Poly*



*Metal 1*



*Metal 2*



*Metal 3*

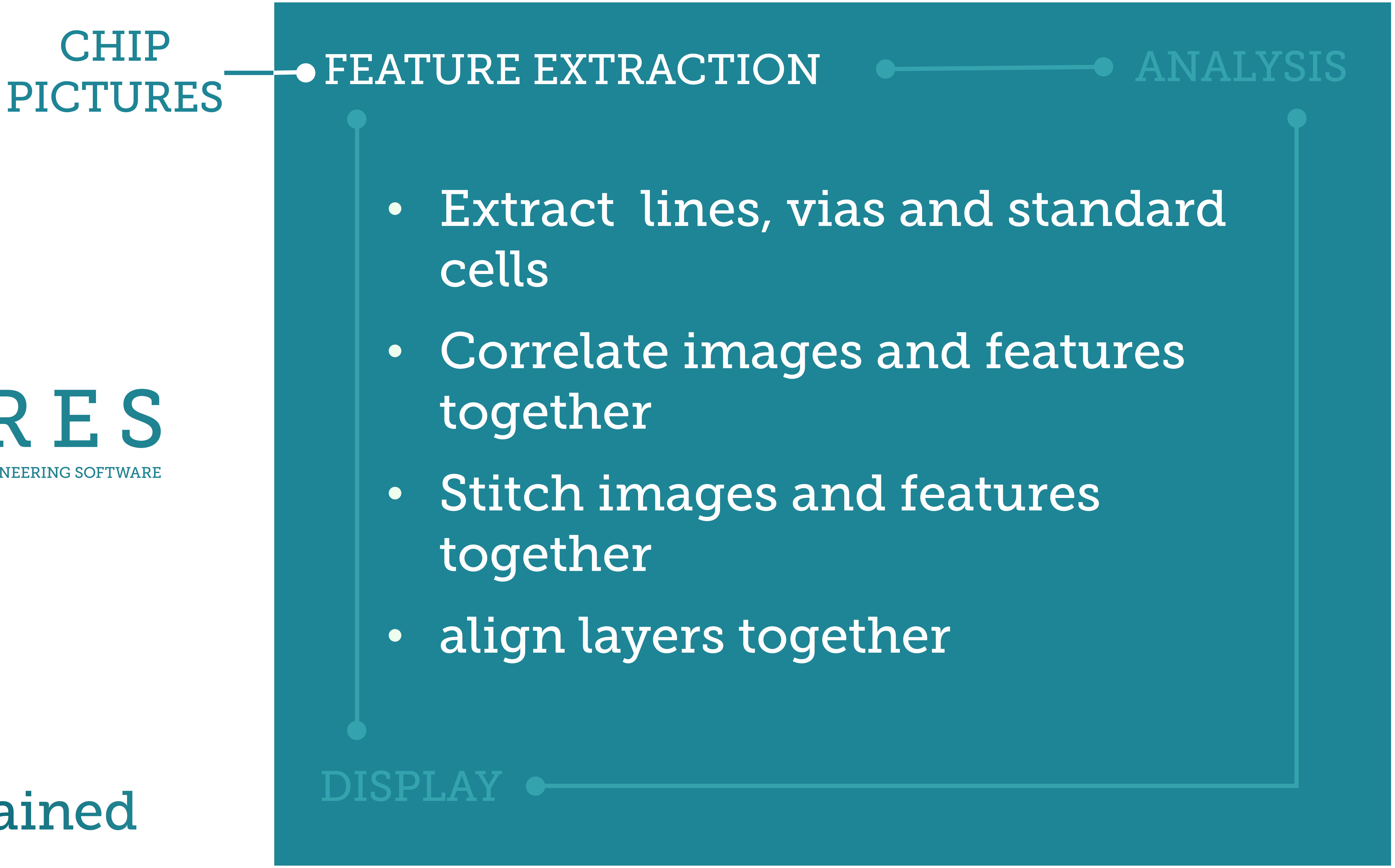
# Analysis

Secure IC

Assisted

- SEM pictures are distorted
- Issue for correlating and stitching large scans
- Issue for aligning layers
- Tracing signal inside the core is mandatory for secure ICs
- Thousands of gates to reverse and link together

# Analysis



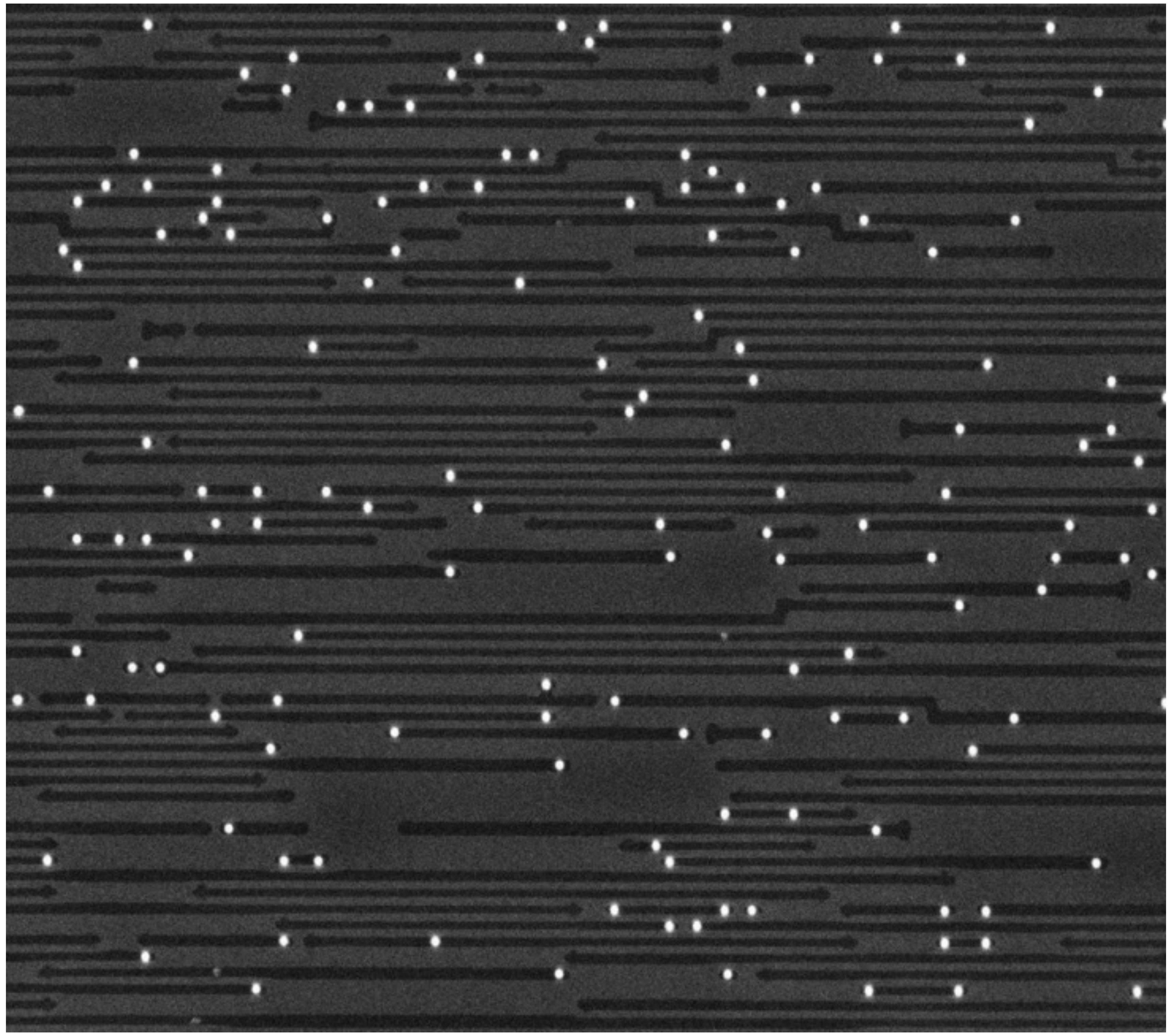
- Extract  lines, vias and standard cells
- Correlate images and features together
- Stitch images and features together
- align layers together

ARES

AUTOMATED REVERSE ENGINEERING SOFTWARE

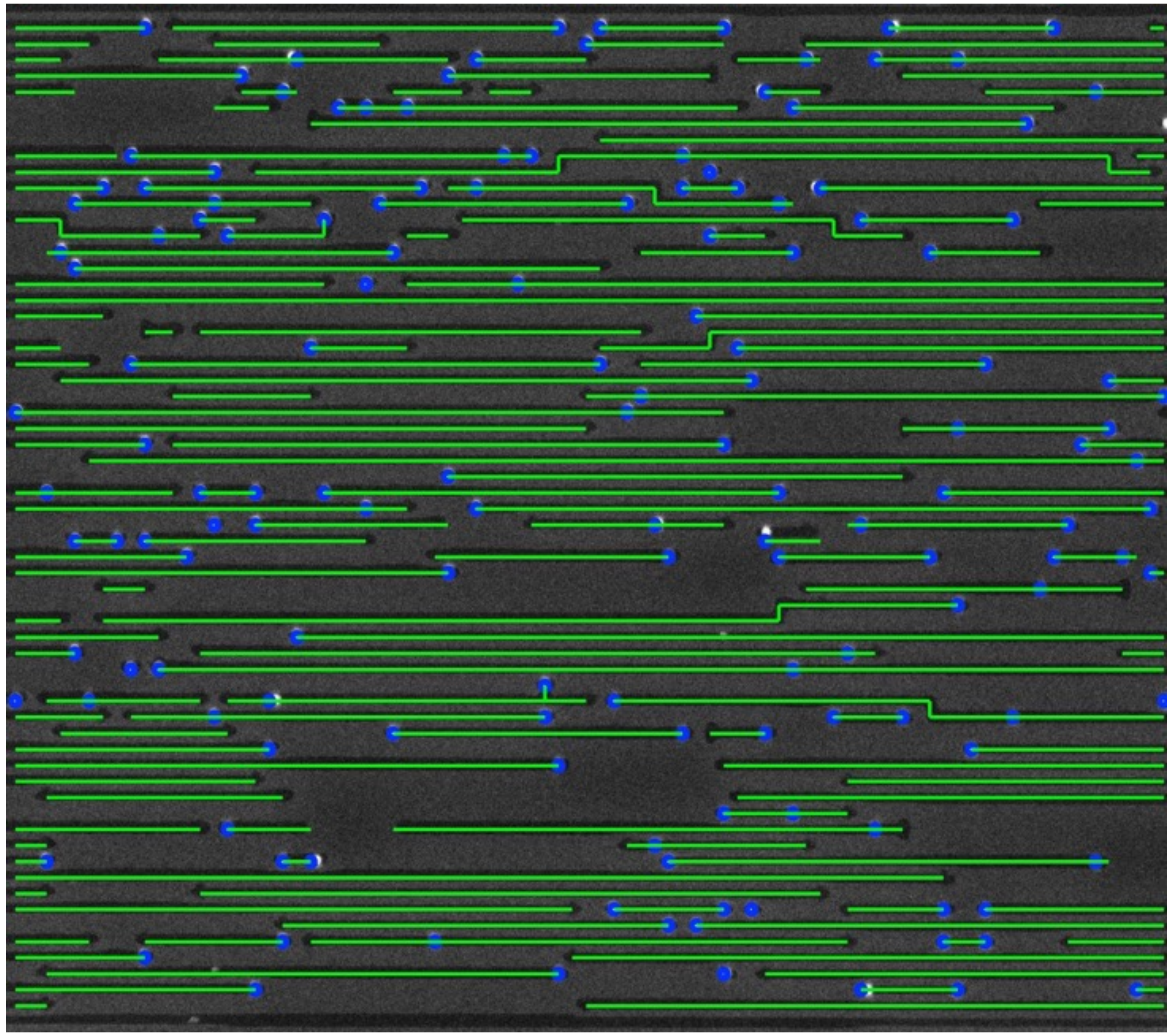
Texplained

# Feature Extraction



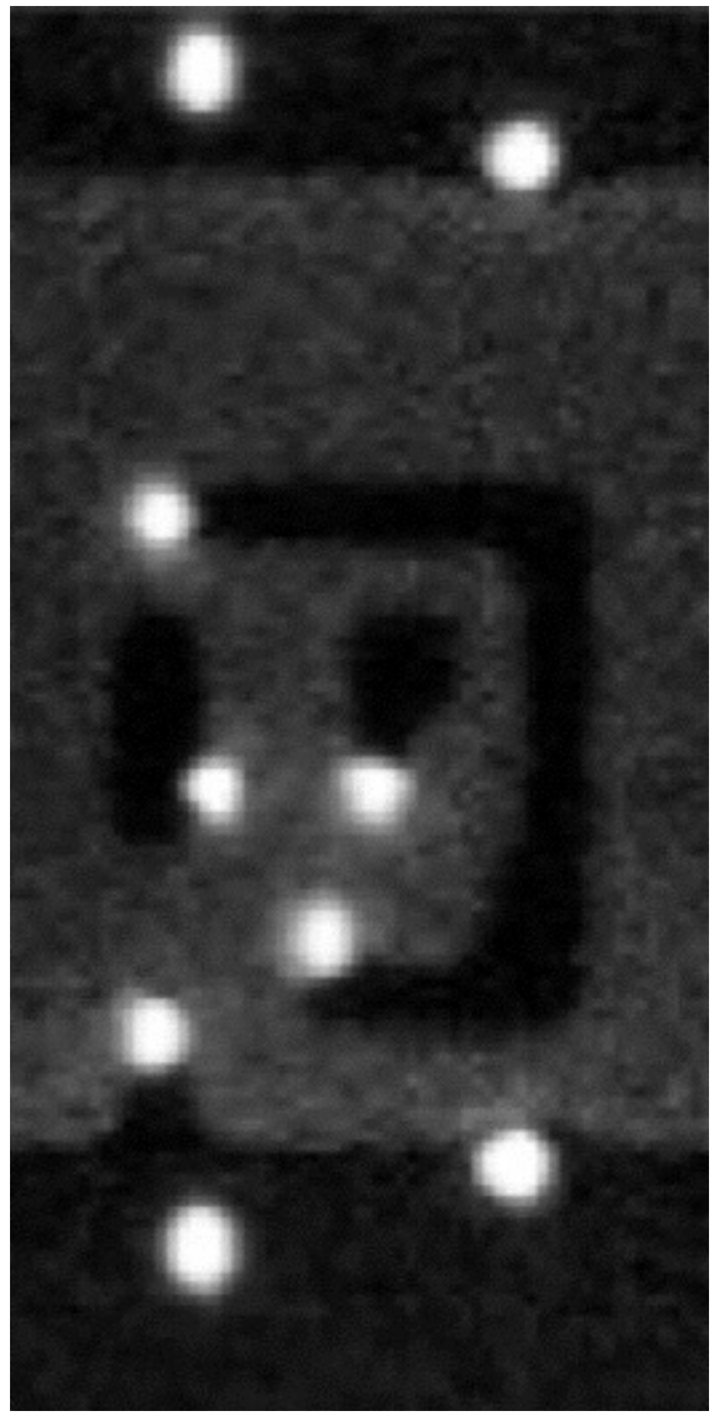
Source Picture

Feature extraction

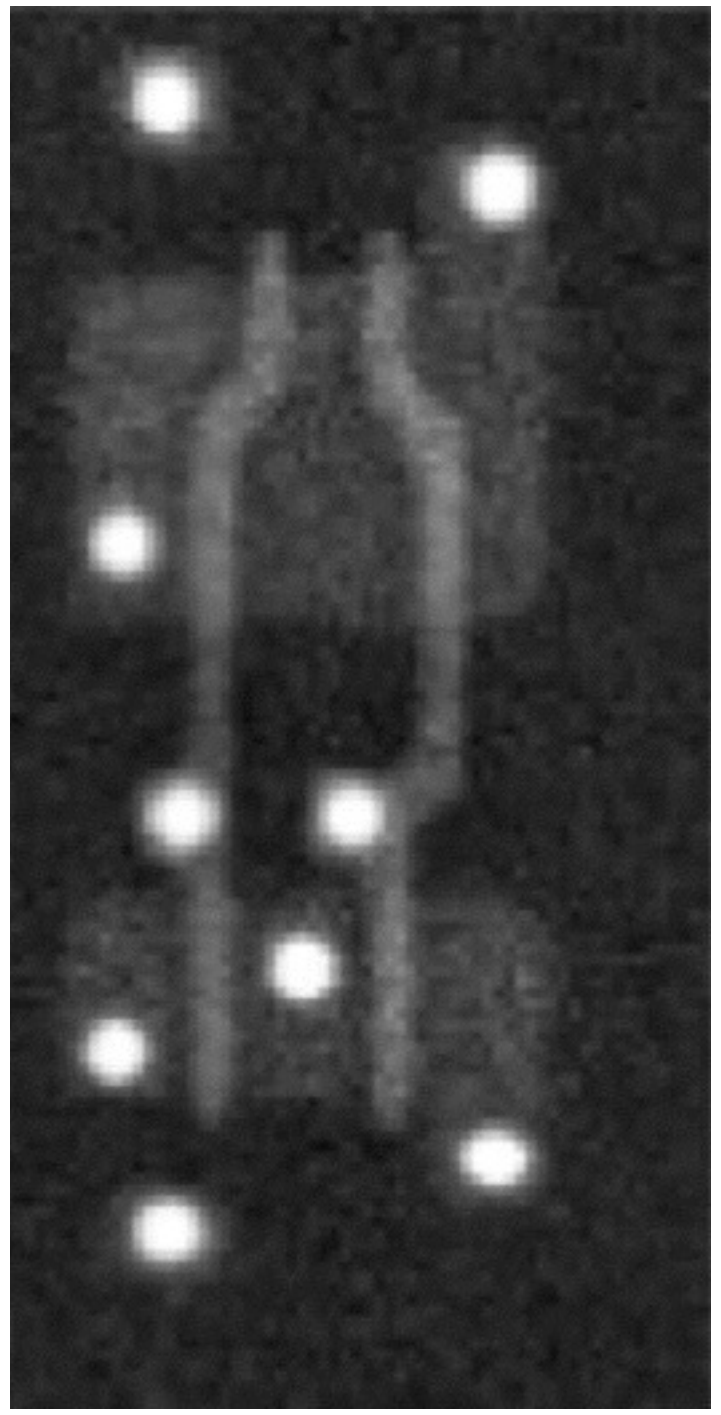


Extracted Lines and Vias

# Feature Extraction

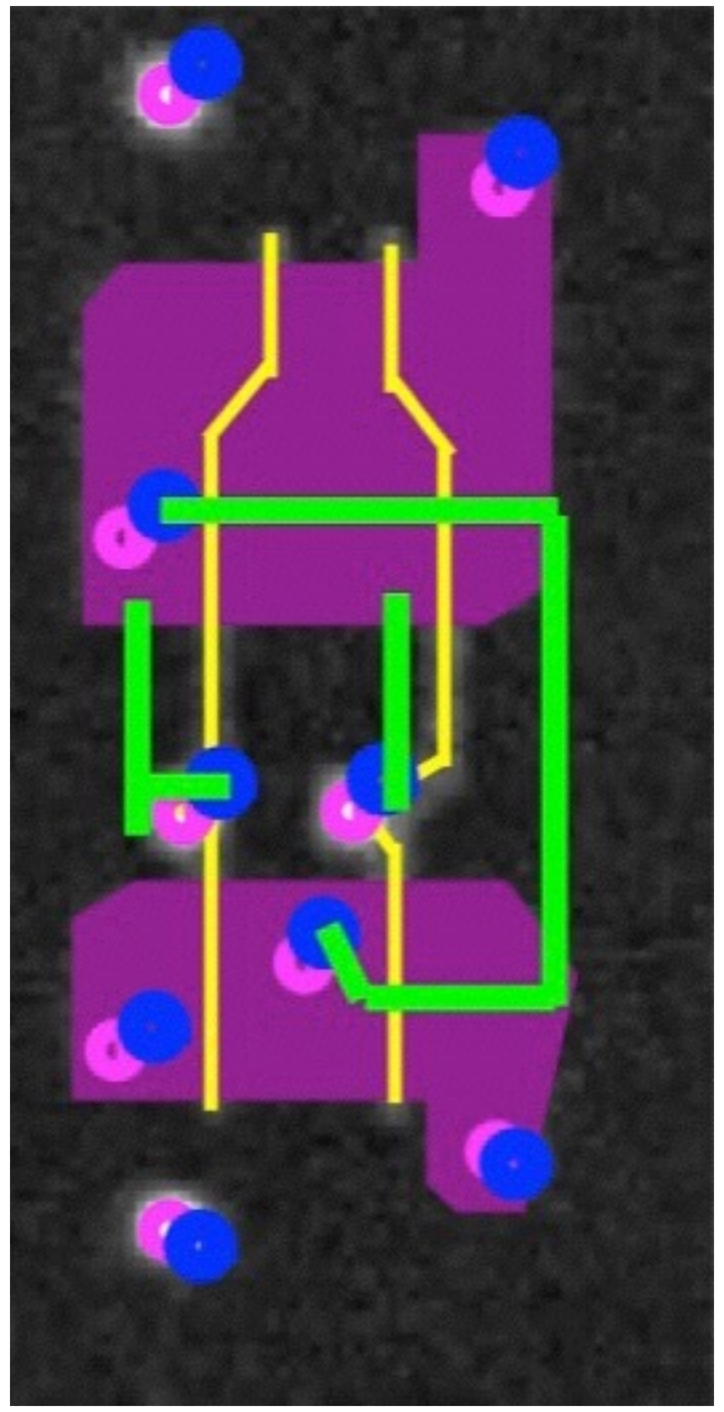


*Metal 1*



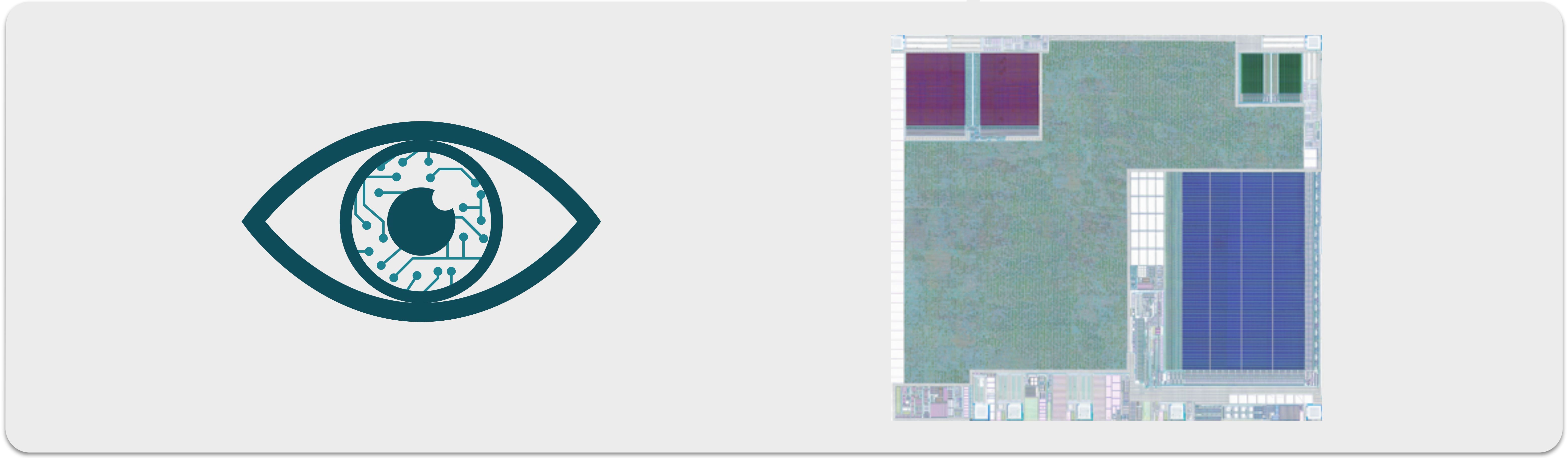
*Poly*

*Feature extraction*



*Extracted Standard Cells*

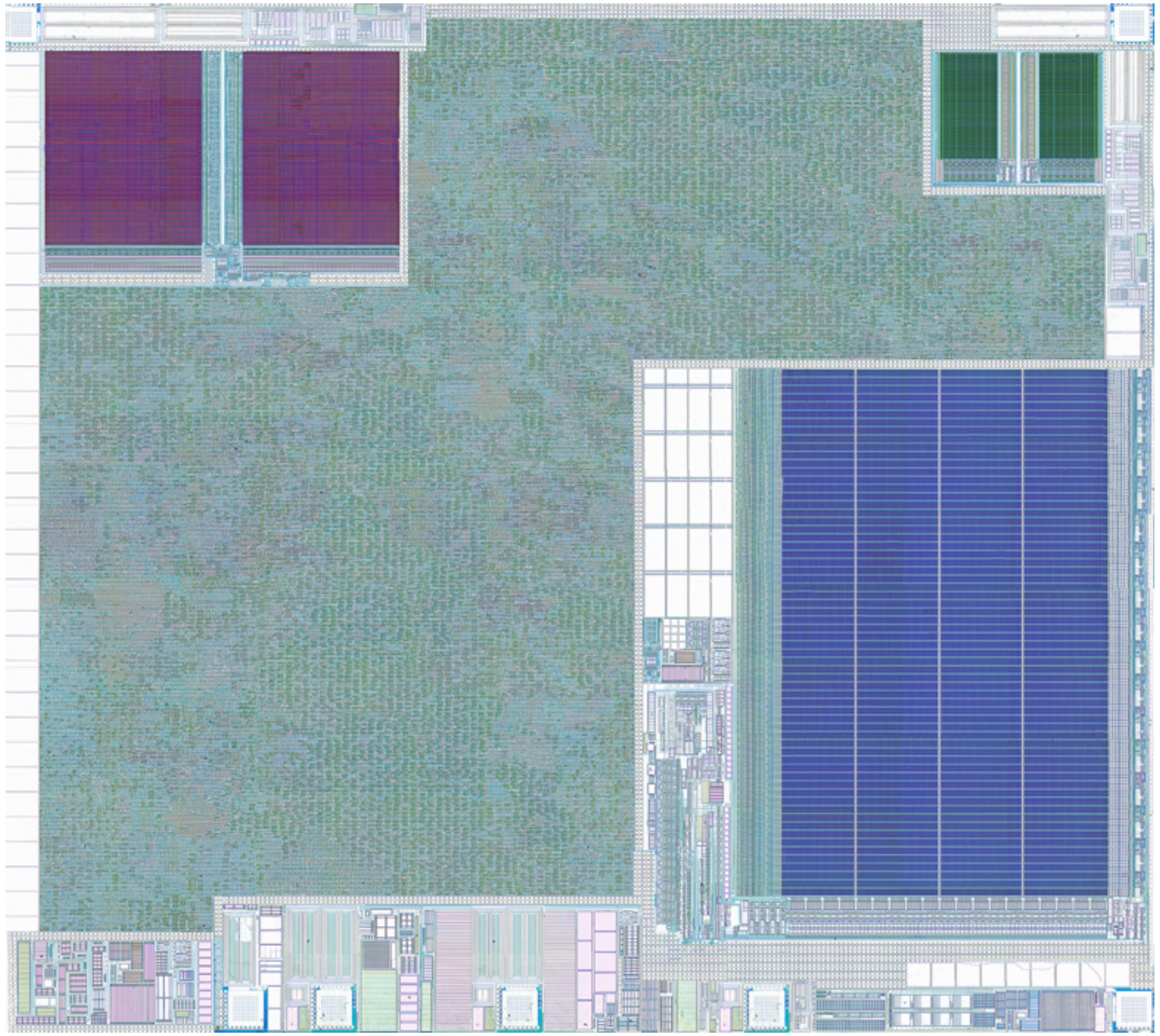
# Overview



Results

# Results

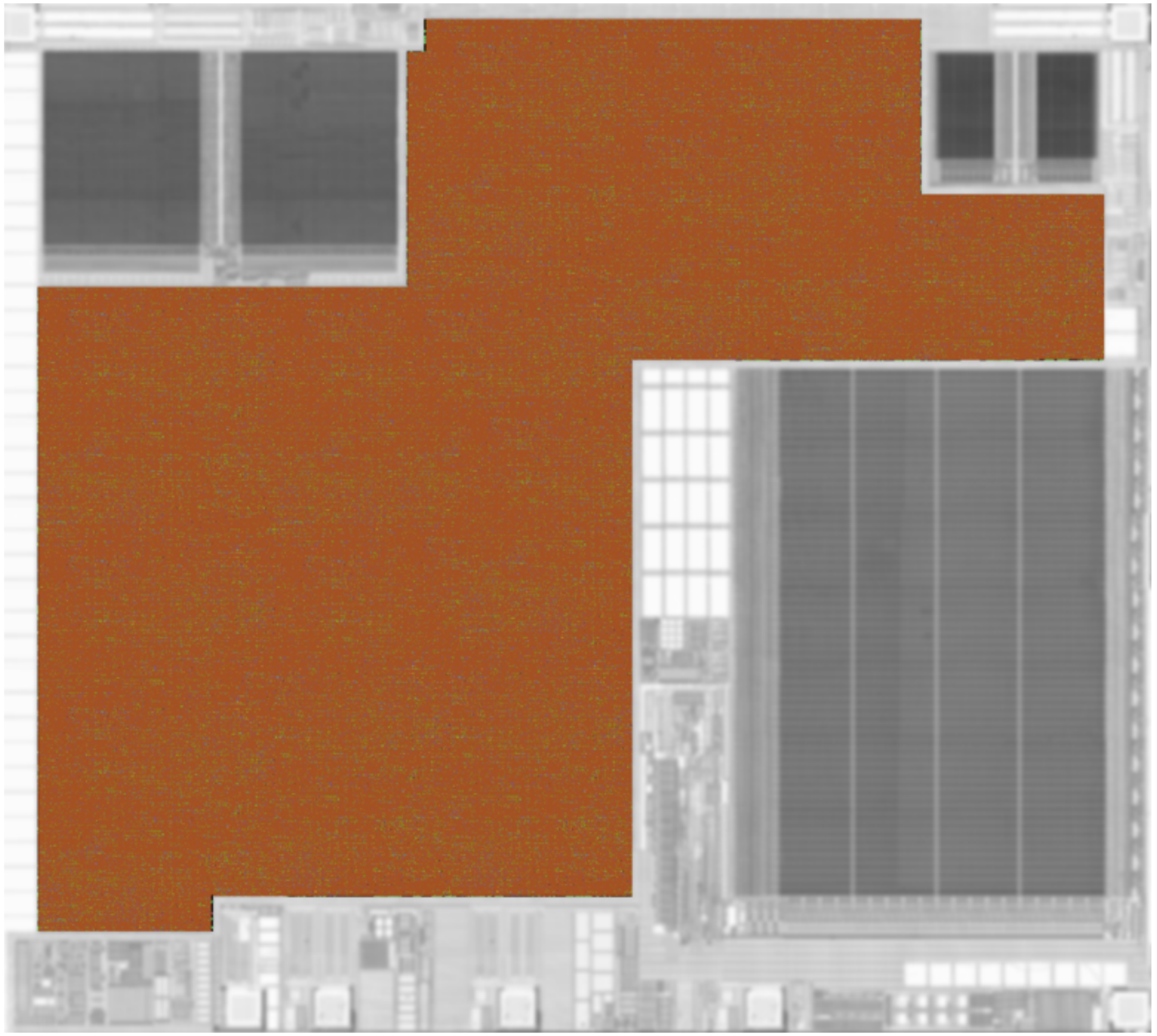
- 2 blocs of RAM
- ROM
- Flash
- Analog blocs
- Core



*Backside Picture*

# Results

- Core will be analyzed
- Lines and Vias are extracted

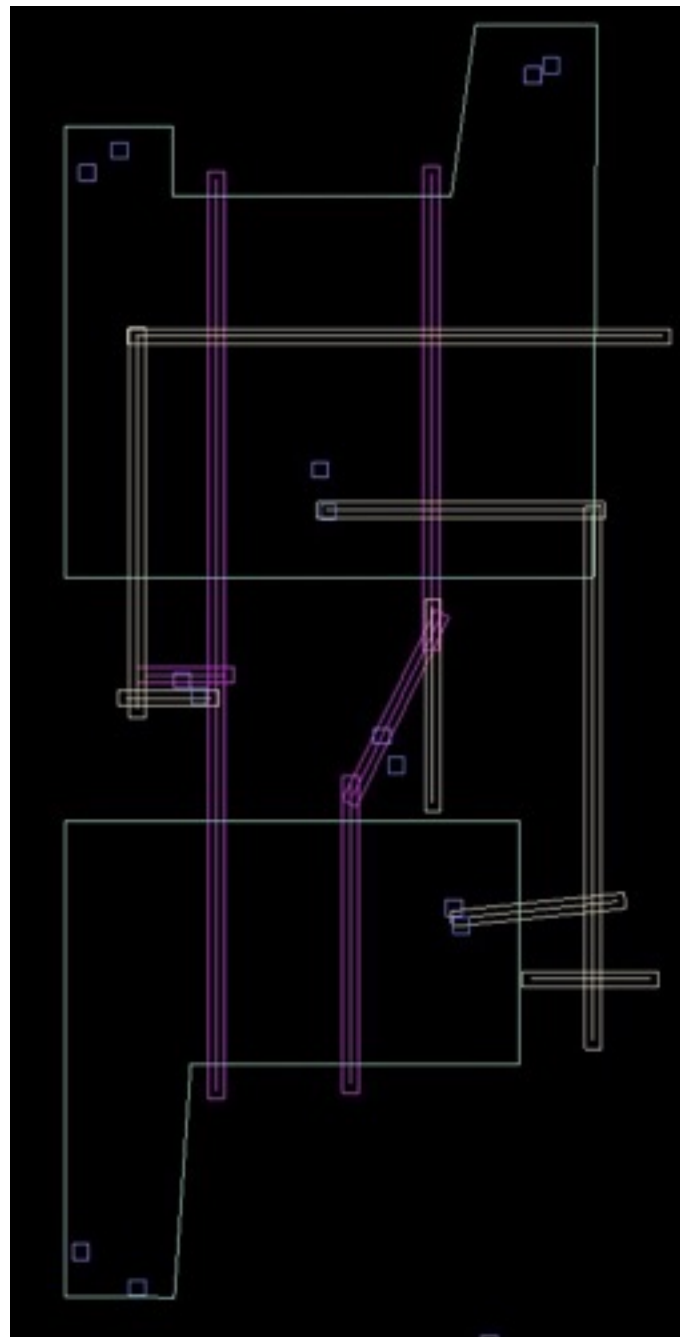


*Extracted Interconnect*

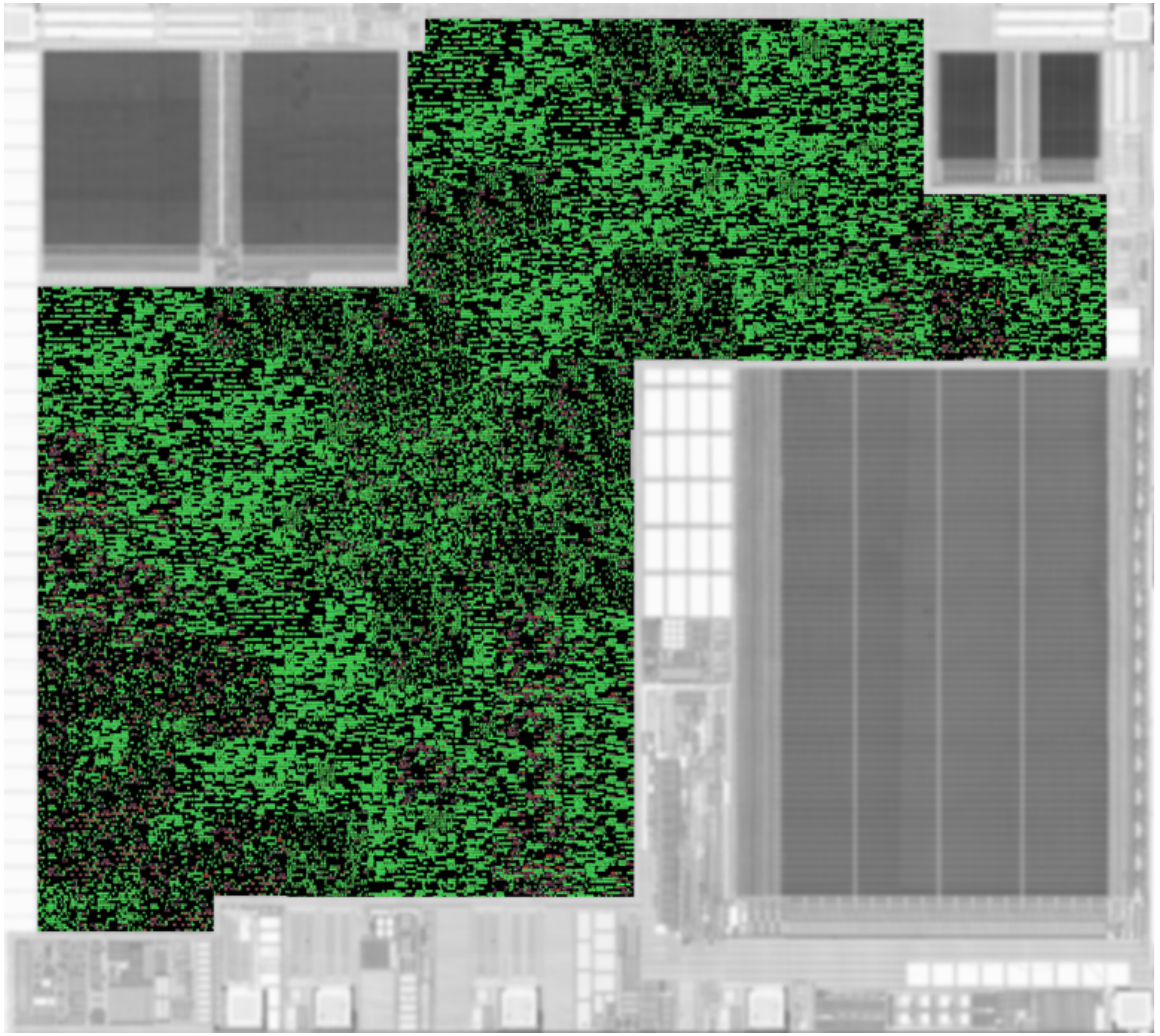
Texplained

# Results

- Standard Cell Library is reconstructed



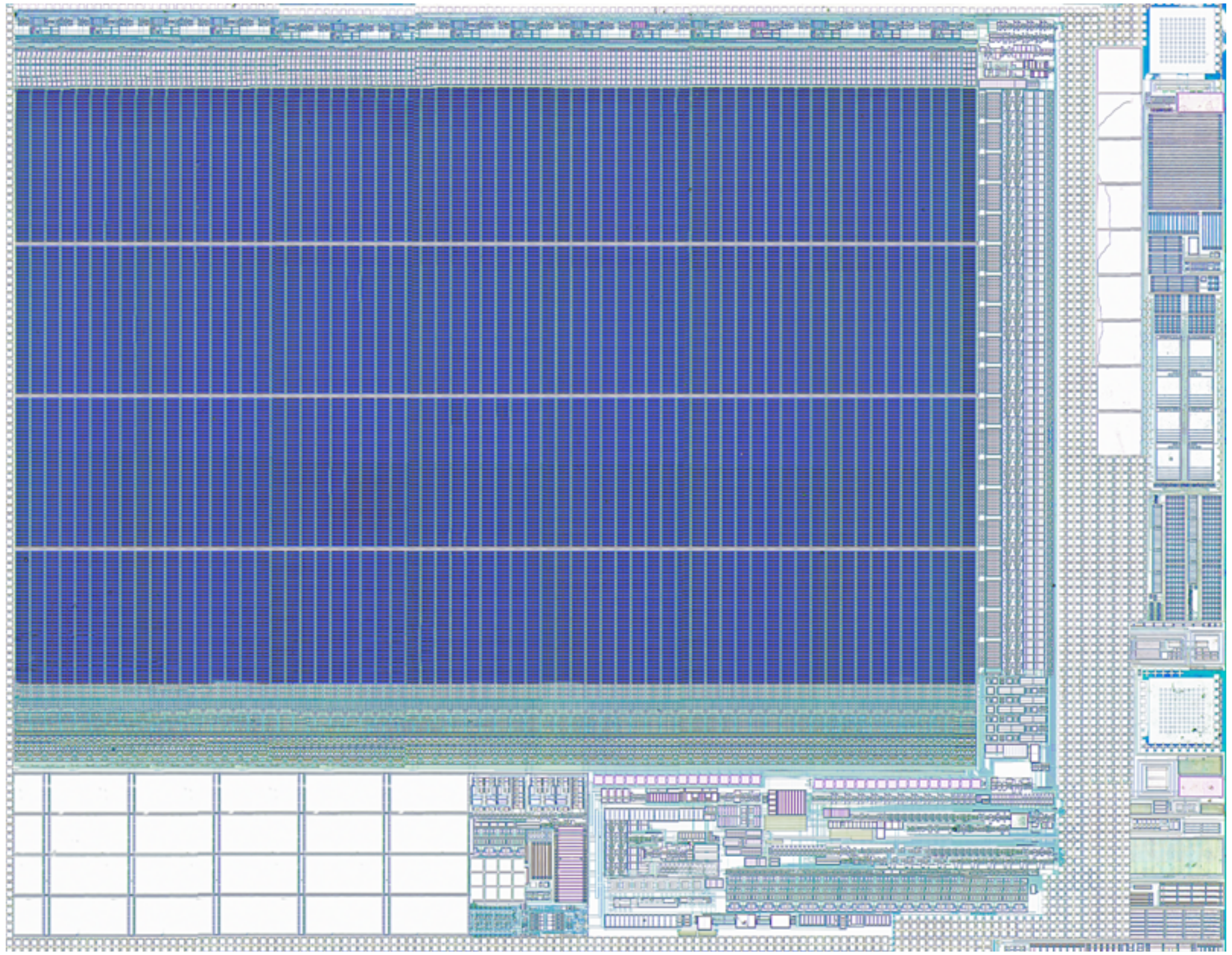
*NAND Gate*



*Extracted Standard Cells*

# Reading The Flash

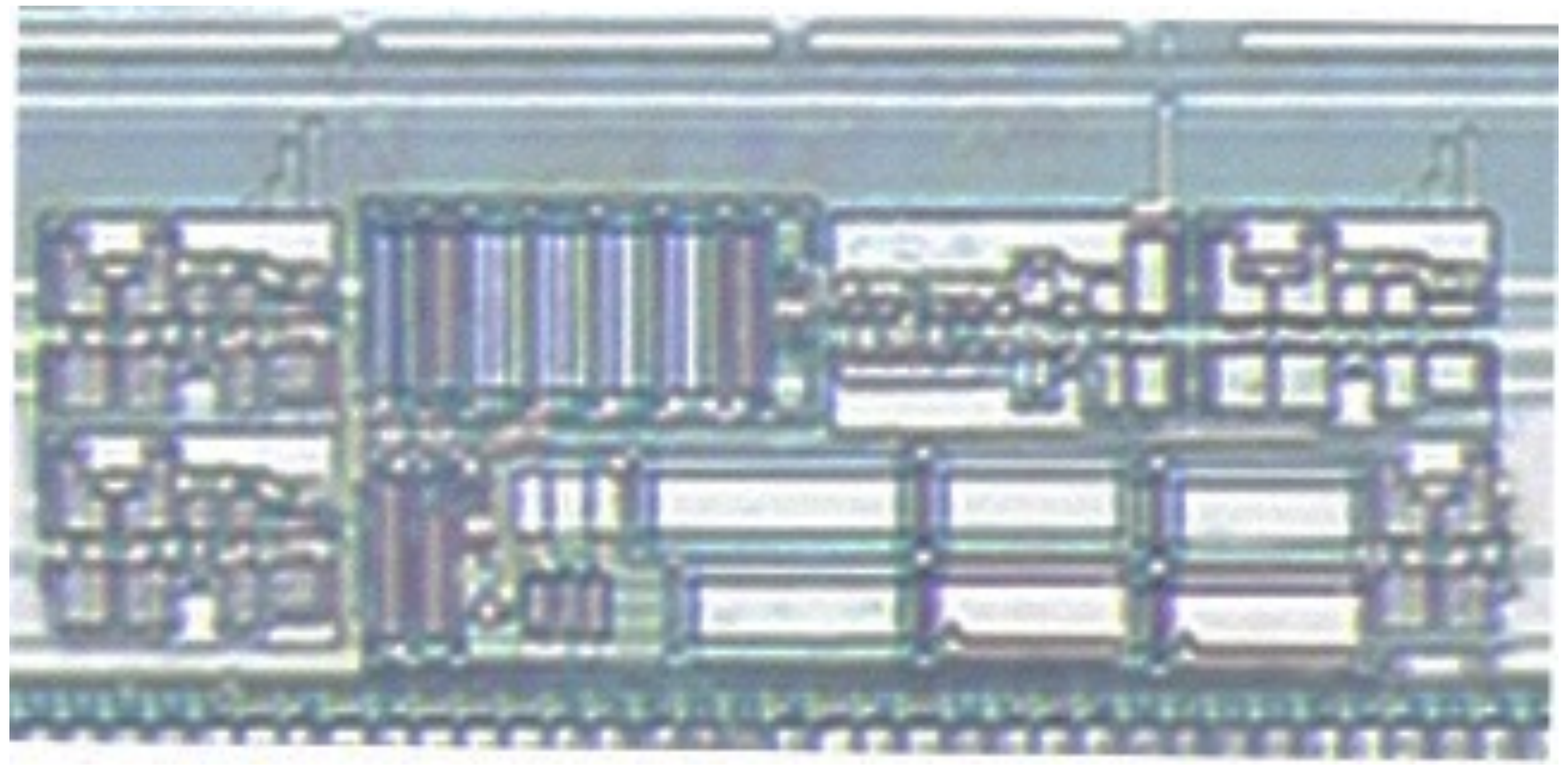
- Flash is easy to spot :
  - Charge pump used to erase it relies on big capacitors
  - Charge pump can be disabled to prevent a flash erase in case of security interrupt.



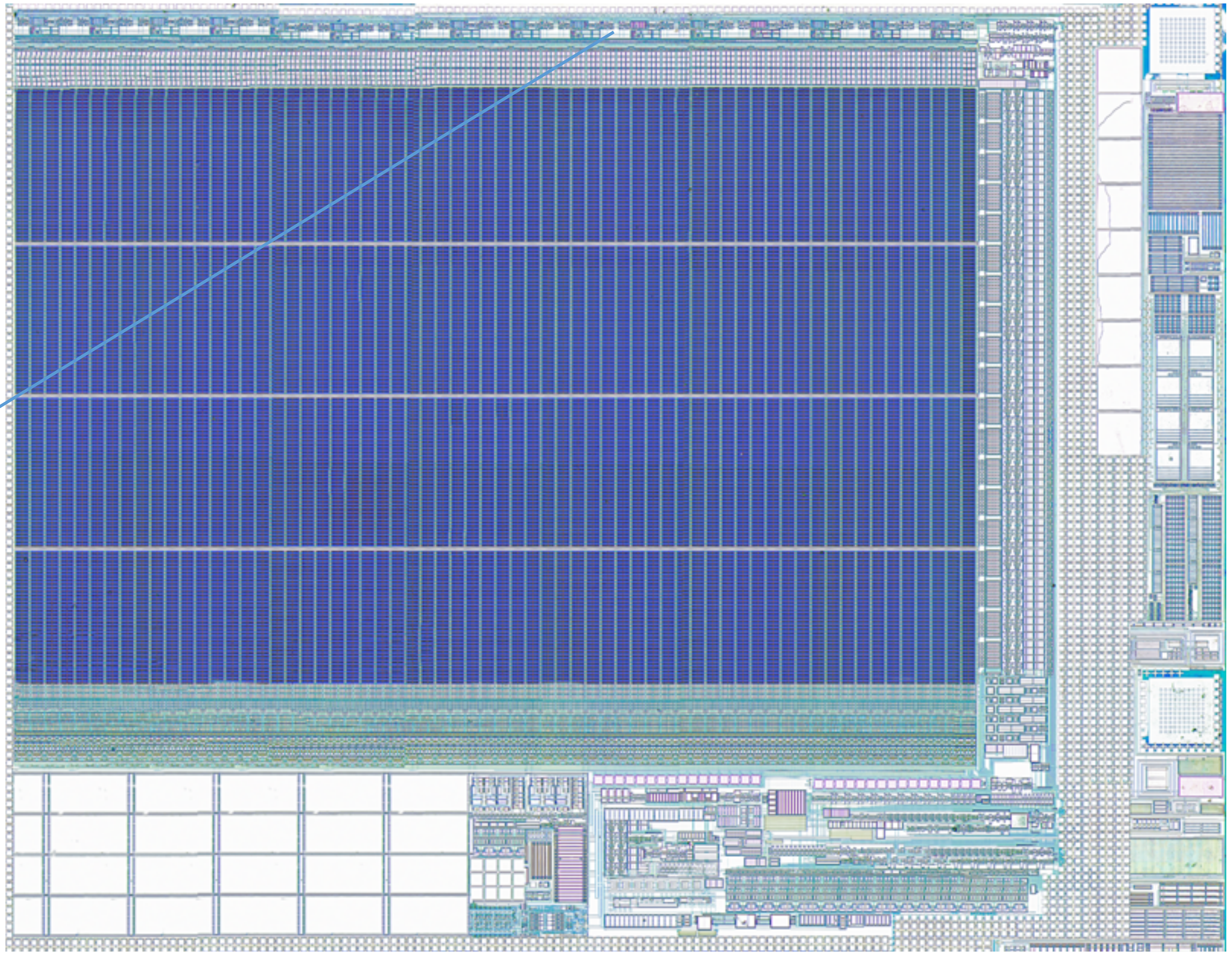
*Flash Memory*

# Reading The Flash

- Flash output buffers are directly visible from the backside
- Output lines get separated in 2 groups that travel along the flash to the core.



*Flash Output Buffer*

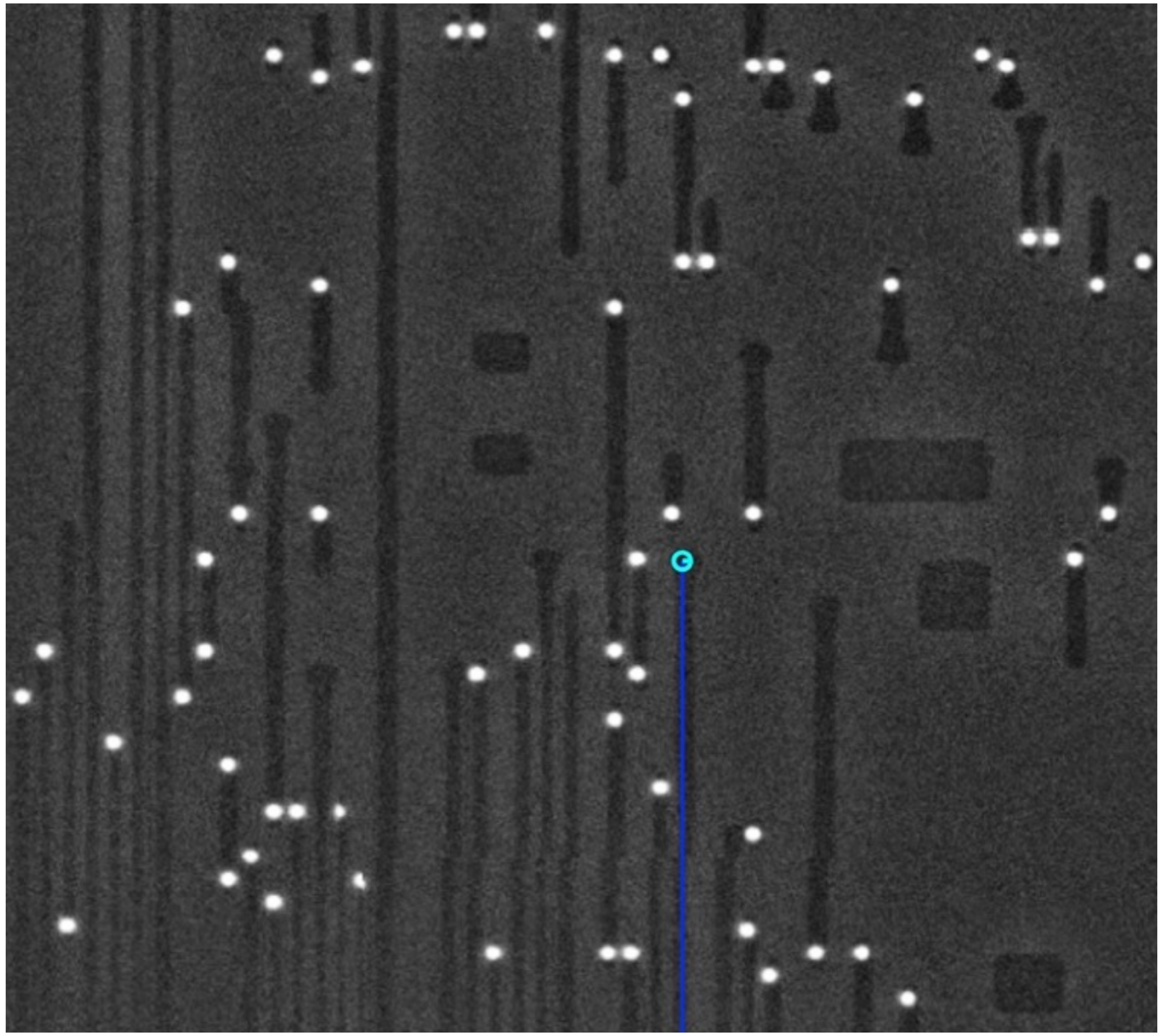


*Flash Memory*

Texplained

# Reading The Flash

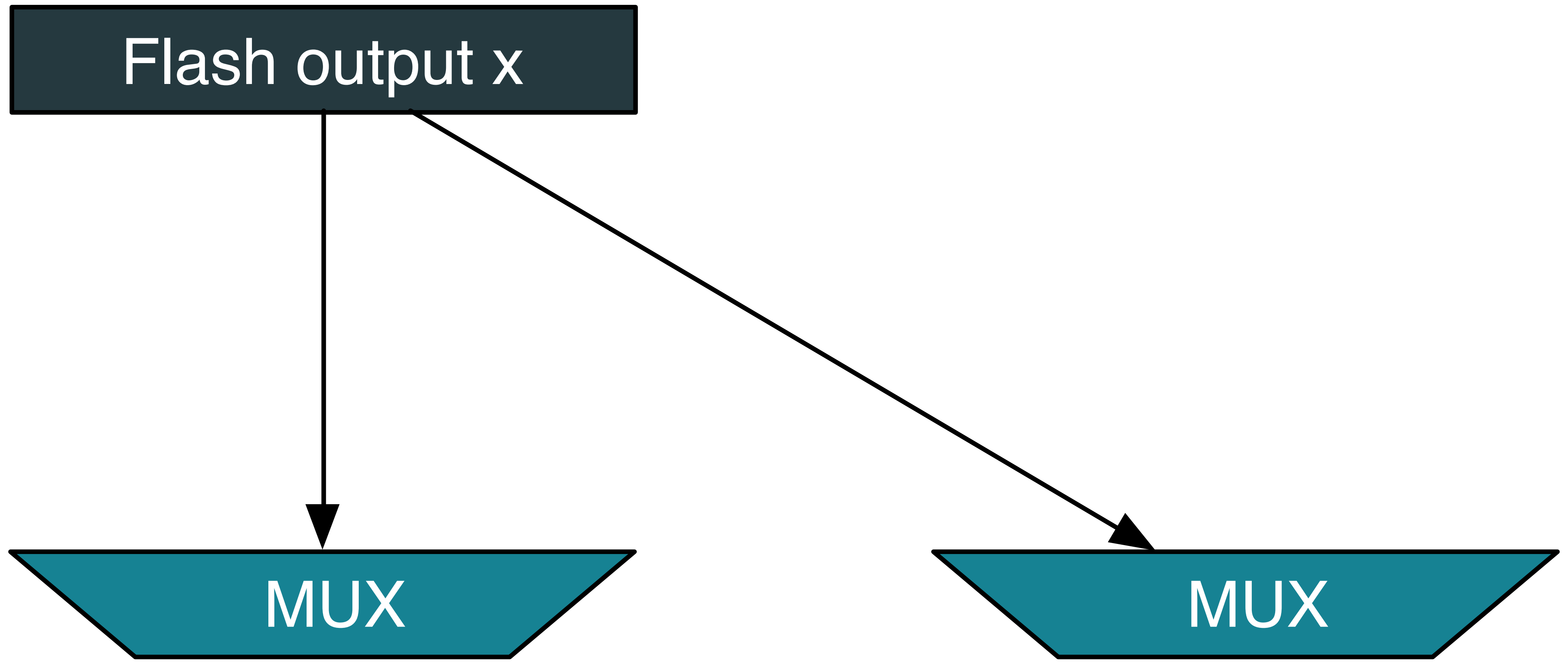
- Only one of the flash output could be traced to the core.
- Position of the other output is approximative.

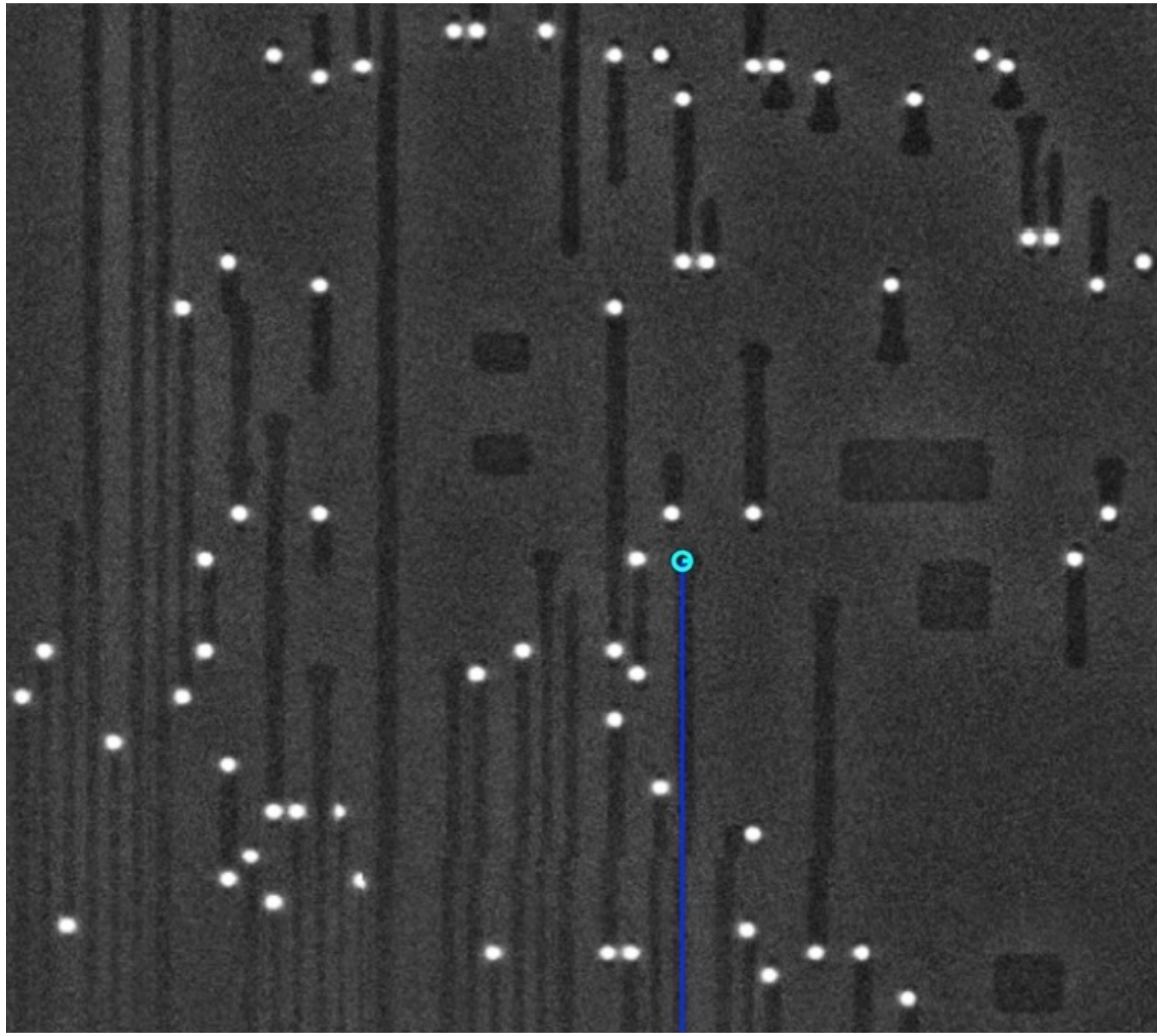


*Flash output going inside the core*

# Reading The Flash

- Tracing the known flash output leads to 2 multiplexers.

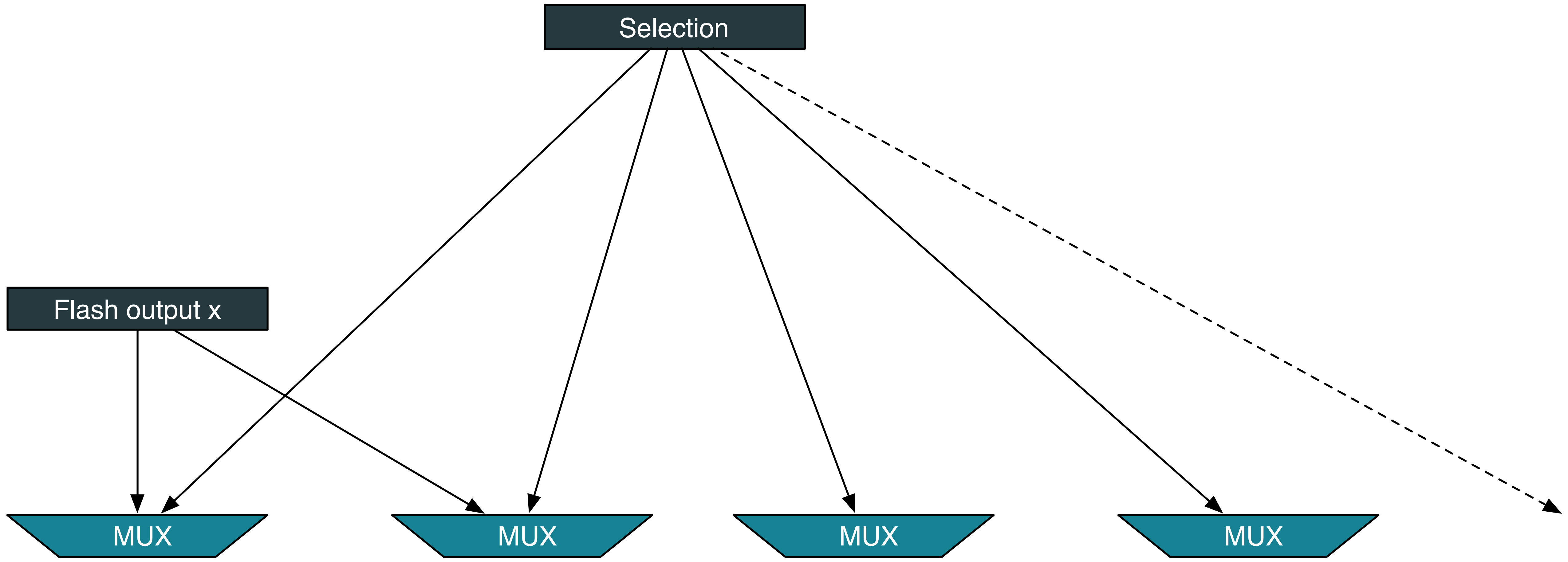


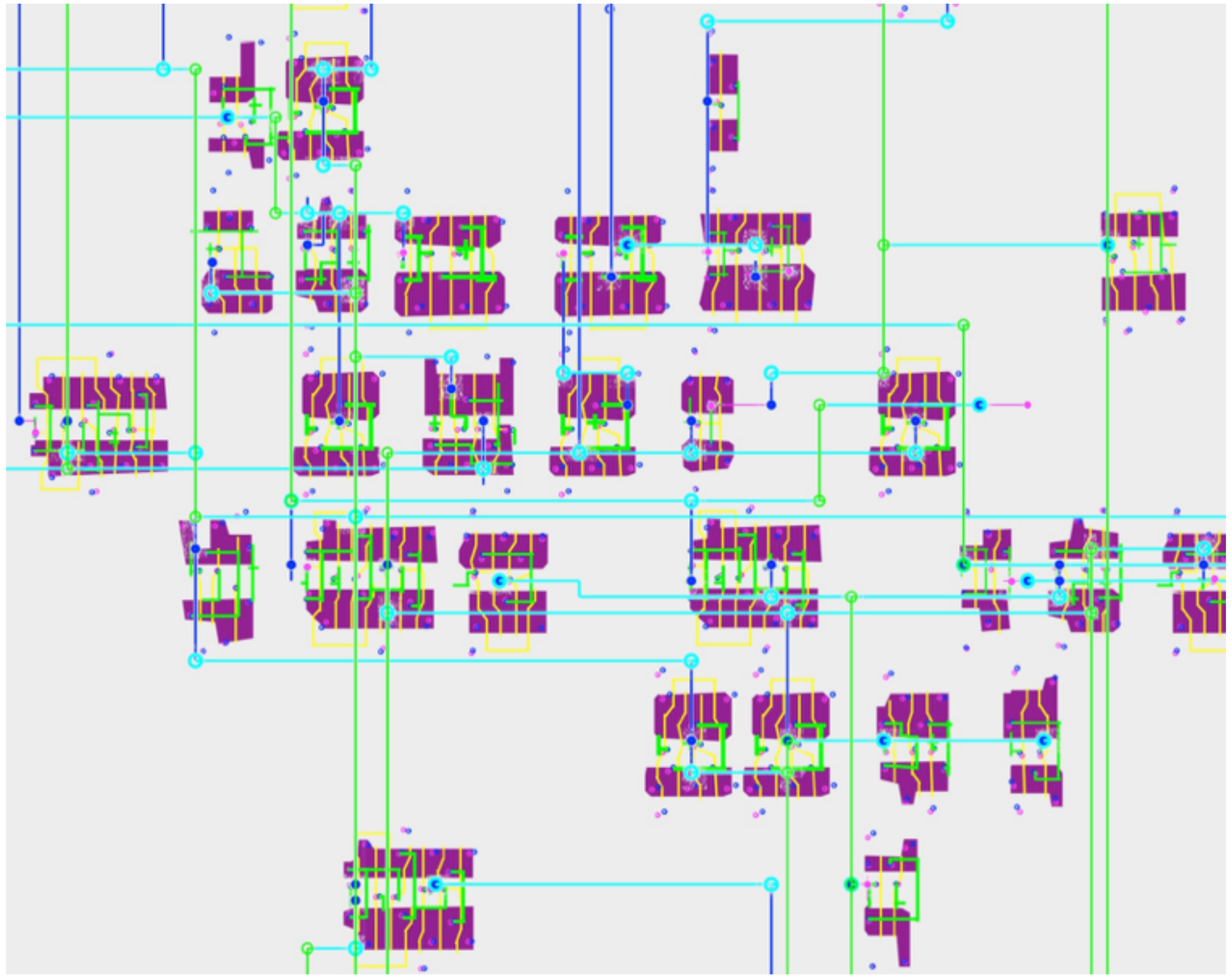


*Flash output going inside the core*

# Reading The Flash

- Tracing the selection signal of the multiplexer shows that the bus must be multiplexed.

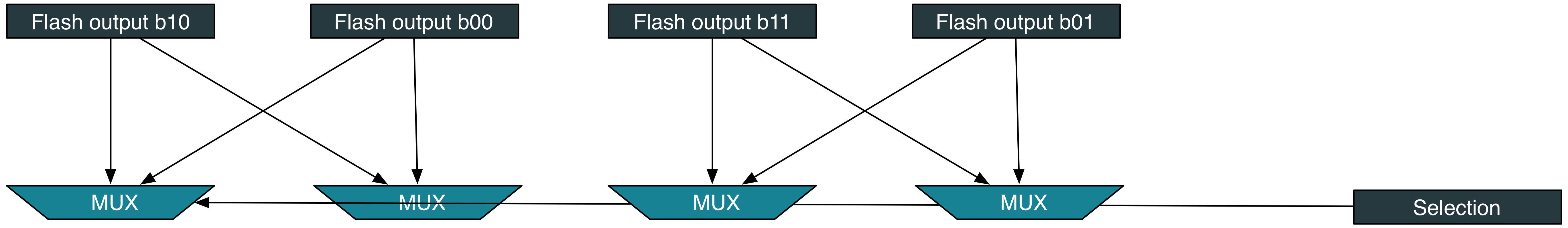


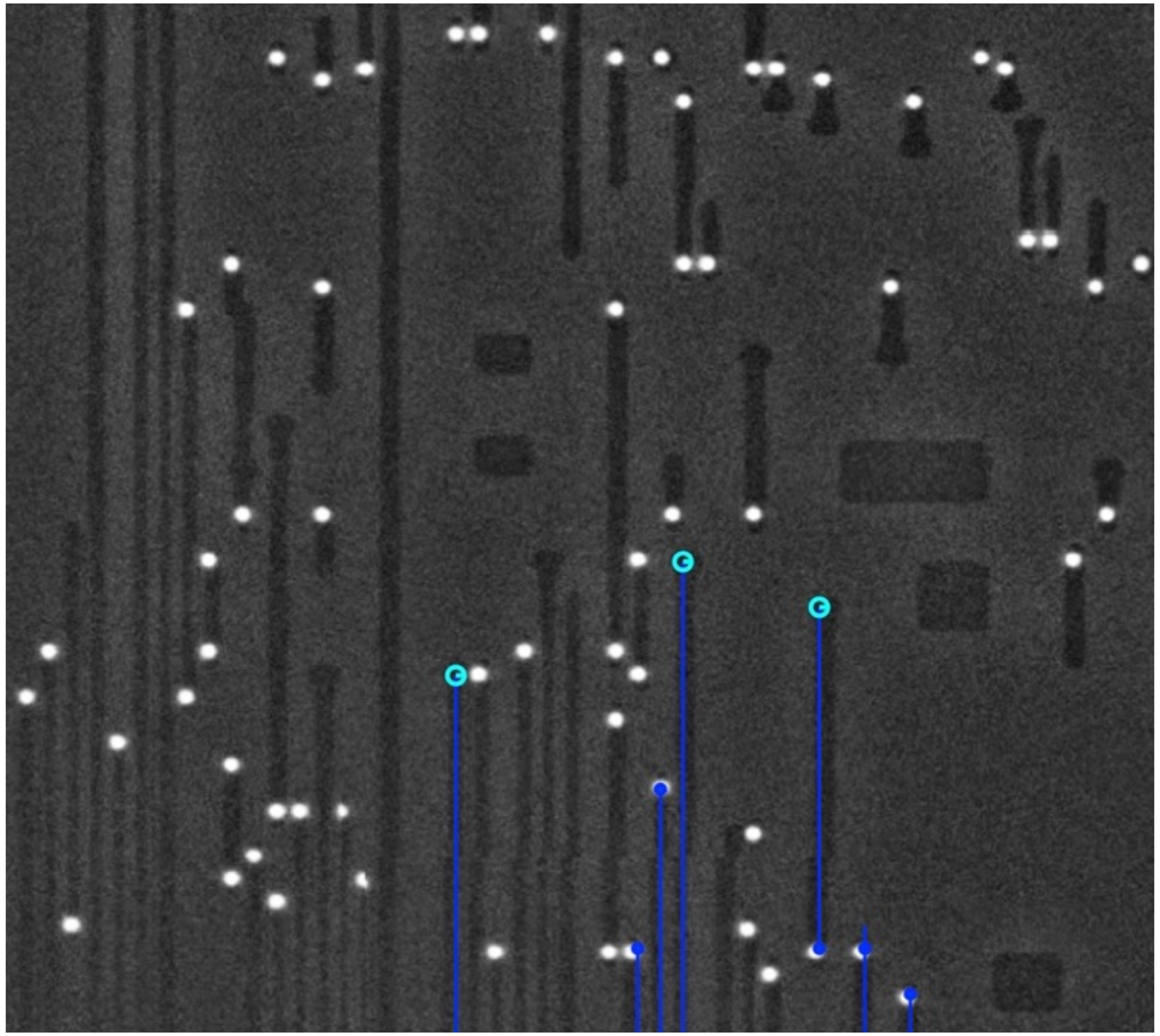


*Traced signals and their connected standard cells*

# Reading The Flash

- Tracing back from the multiplexers confirms the position of the other flash outputs.
- It also shows that bytes can be handled in different orders (endianness…)

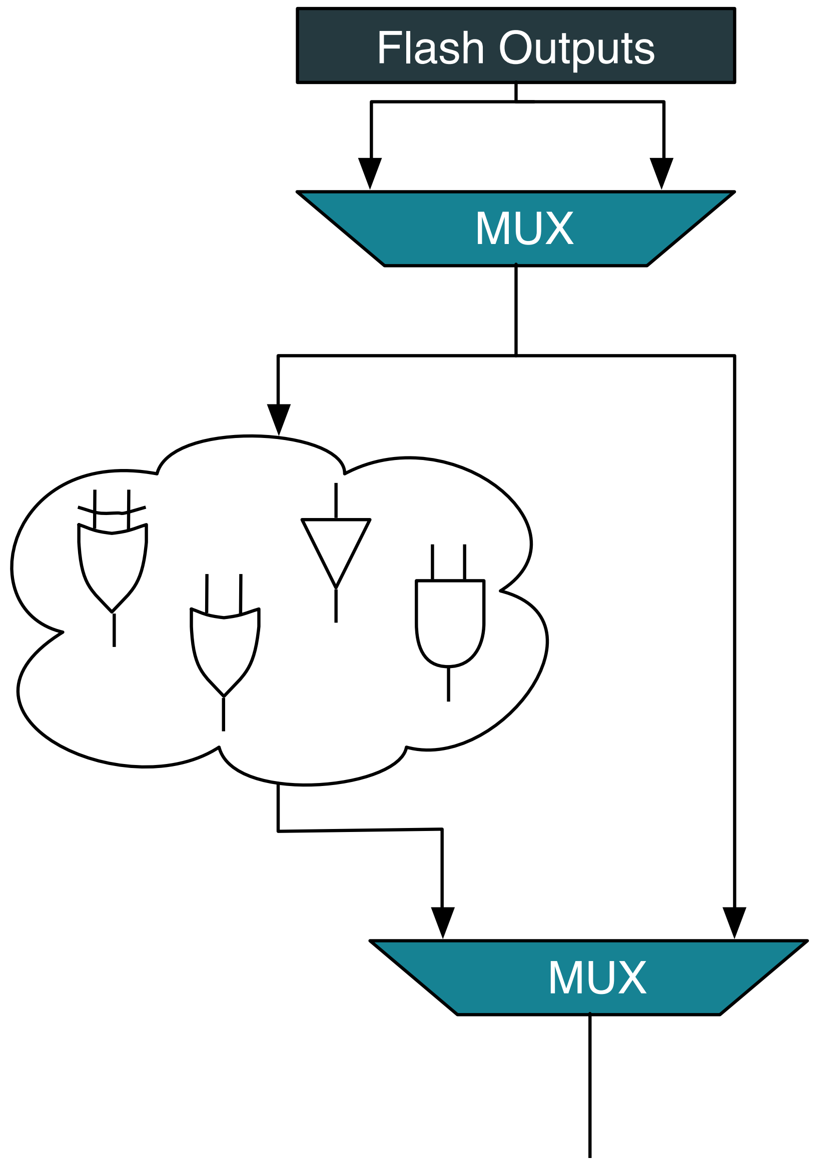


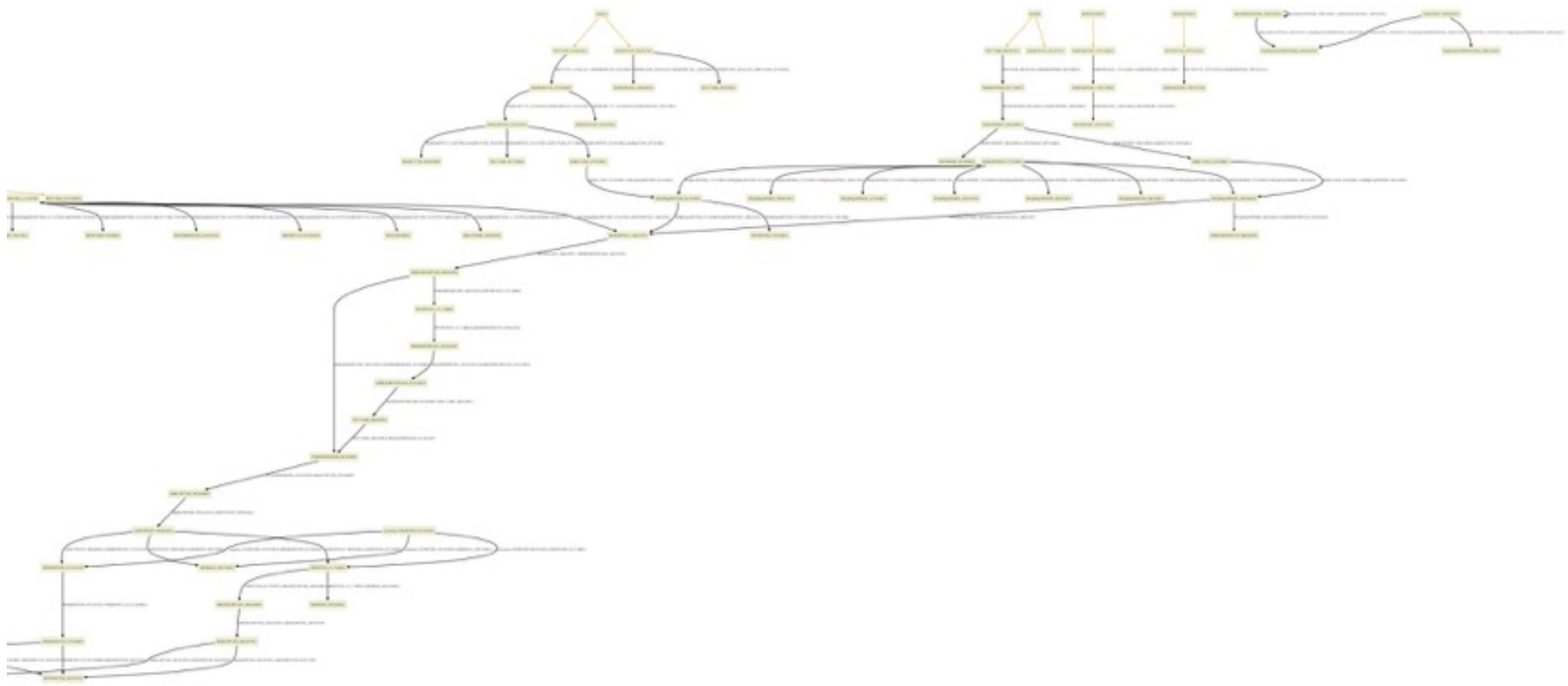


*6 flash outputs*

# Reading The Flash

- Next step is finding the Instruction Register
- 2 data paths.





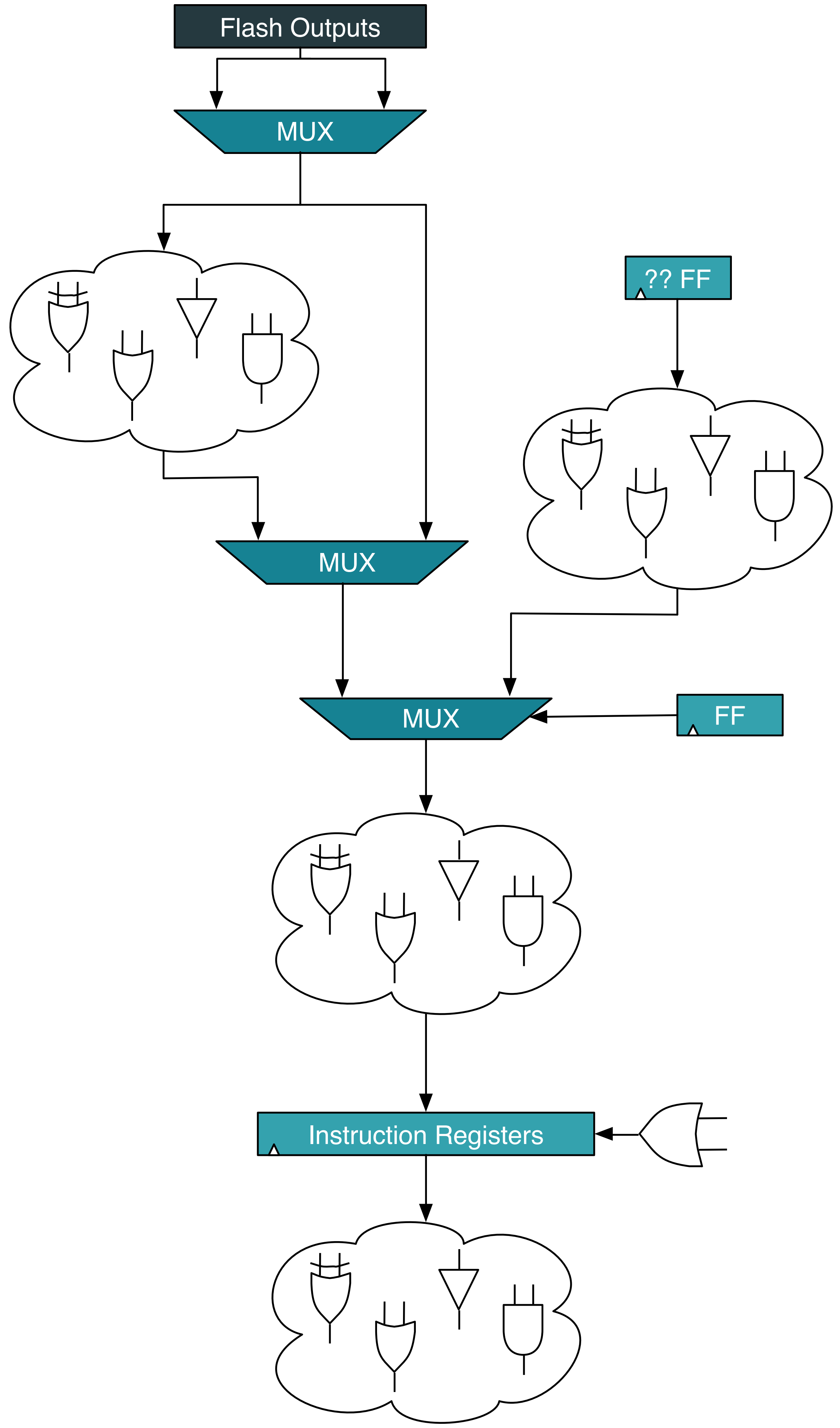
*ARES net tracing visualization.*

Texplained

# Reading The Flash

- First group of Flip-Flops found.
- It could be the Instruction Register
- Following bloc would be the Instruction Decoder then.

- Group bits inside the presumed Instruction Decoder
- Compare with the instruction set
- Match between the 2 : IR found



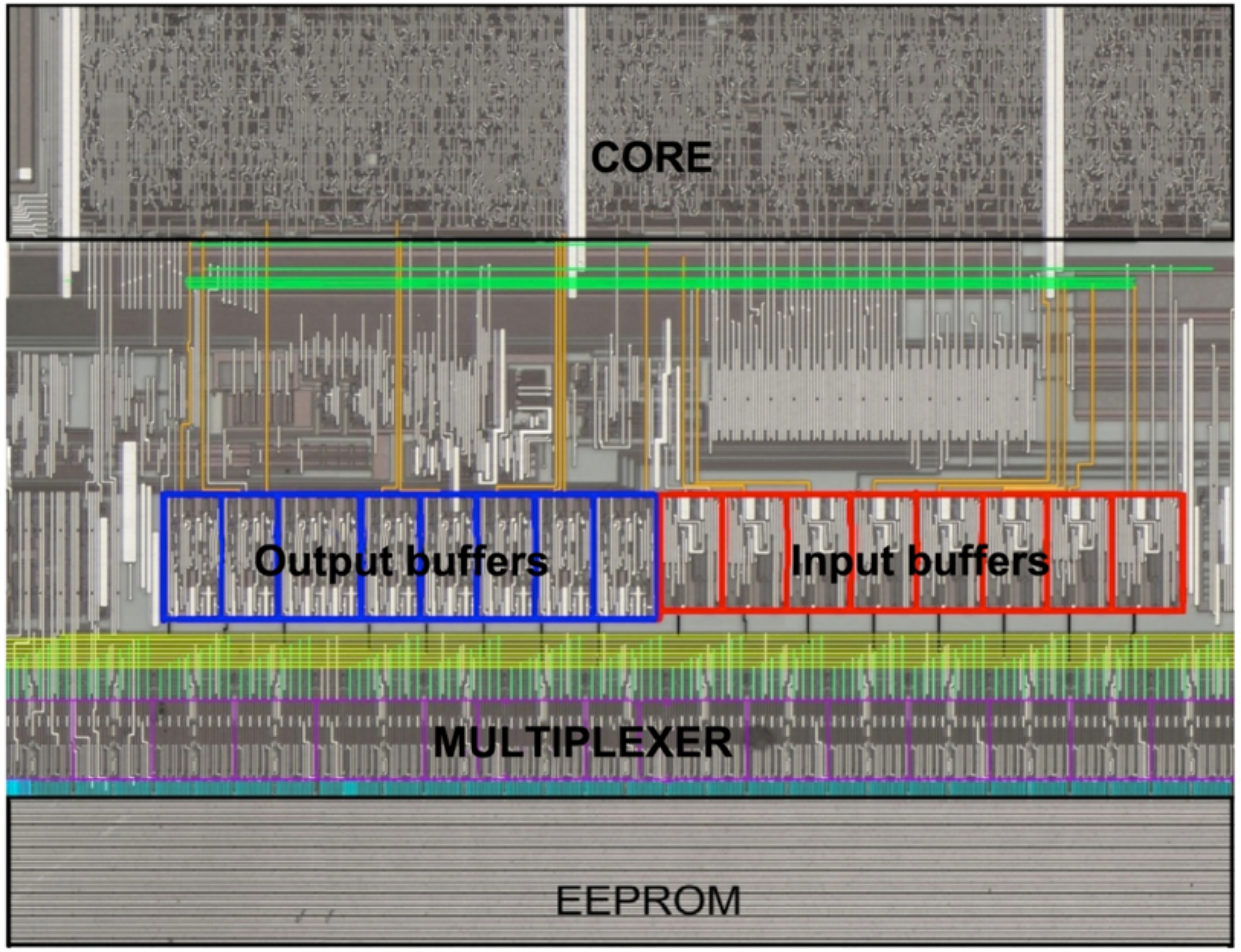
*Flash bus schematic*

# Attack Strategy For Reading The Flash

- Instruction register is made of Flip-Flops that have 2 interesting signals:
    - clk / read signal that can be used to synchronize data as some clk cycles may be suppressed by embedded counter-measures
    - Enable signal that disconnect the input from the Flip-Flop.
- Redundancy can be obtained by probing 2 data lines at a time (one needle will stay on its line for all the acquisition).
- 4 needles Linear Code Extraction

# Comparison with old ICs

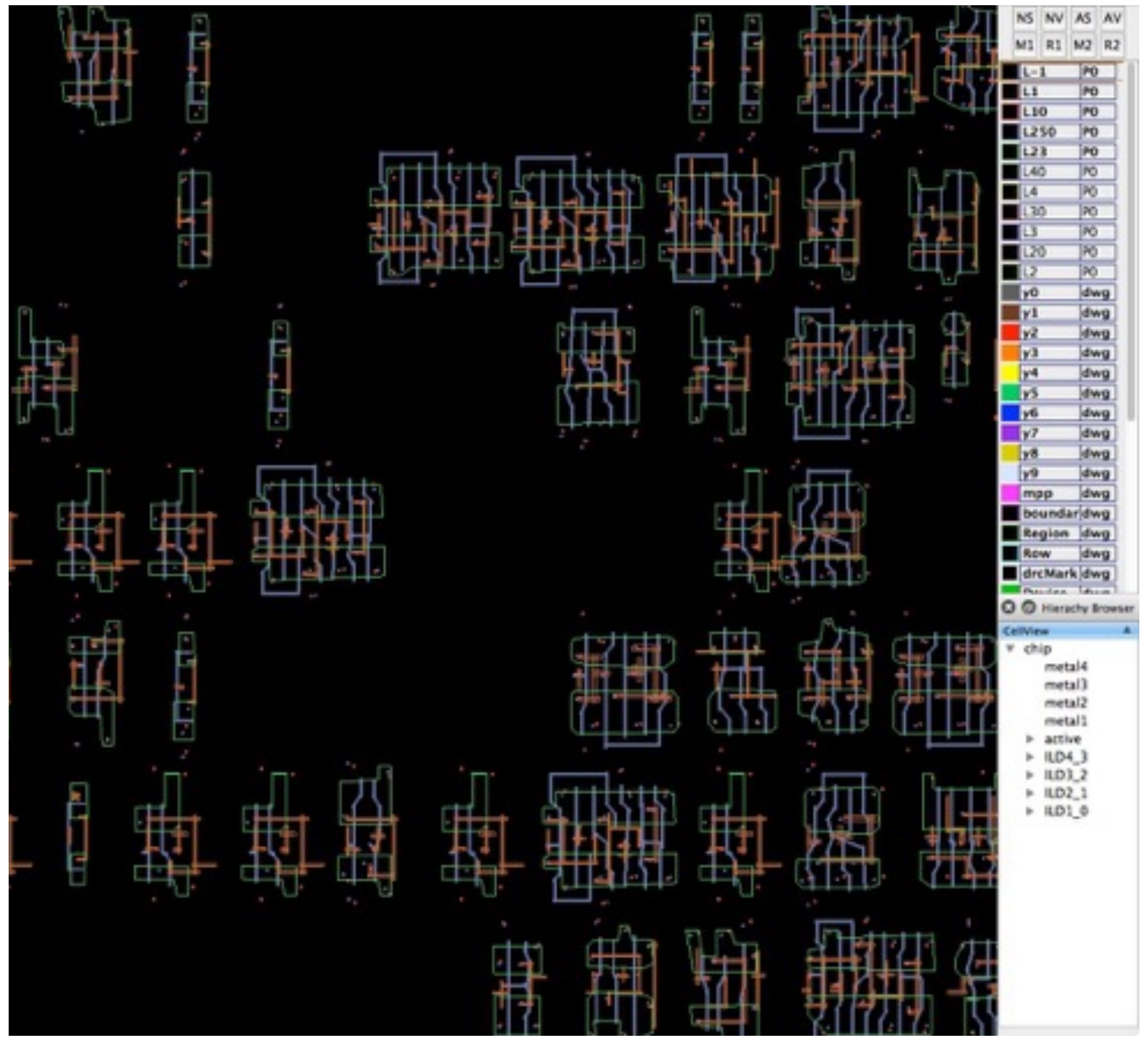
- Linear Code Extraction is still a valid attack scenario.
- Old chips had no protection against it.
- The target hides its bus logic inside a dense core
- This obfuscation does not help when the attacker can fully reverse the core.



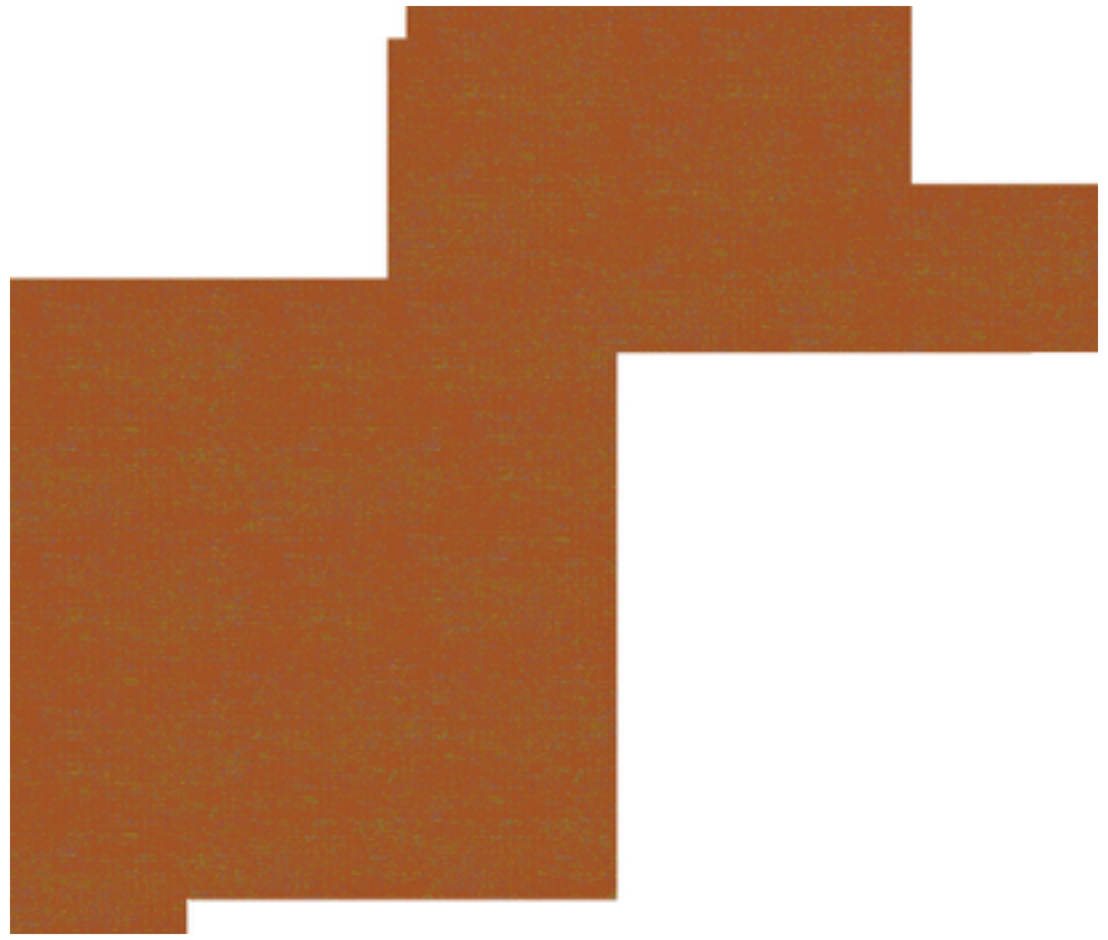
*External Flash Buffers*

# Attack Strategy For Reading The Flash

- Performing the attack can be tricky depending on :
    - shield technology
    - Position of the interesting nets inside the chip (frontside or backside edit)
    - Planarization
- Having all features extracted, a gds2 file has been created. It can be loaded in the FIB for assisted navigation.



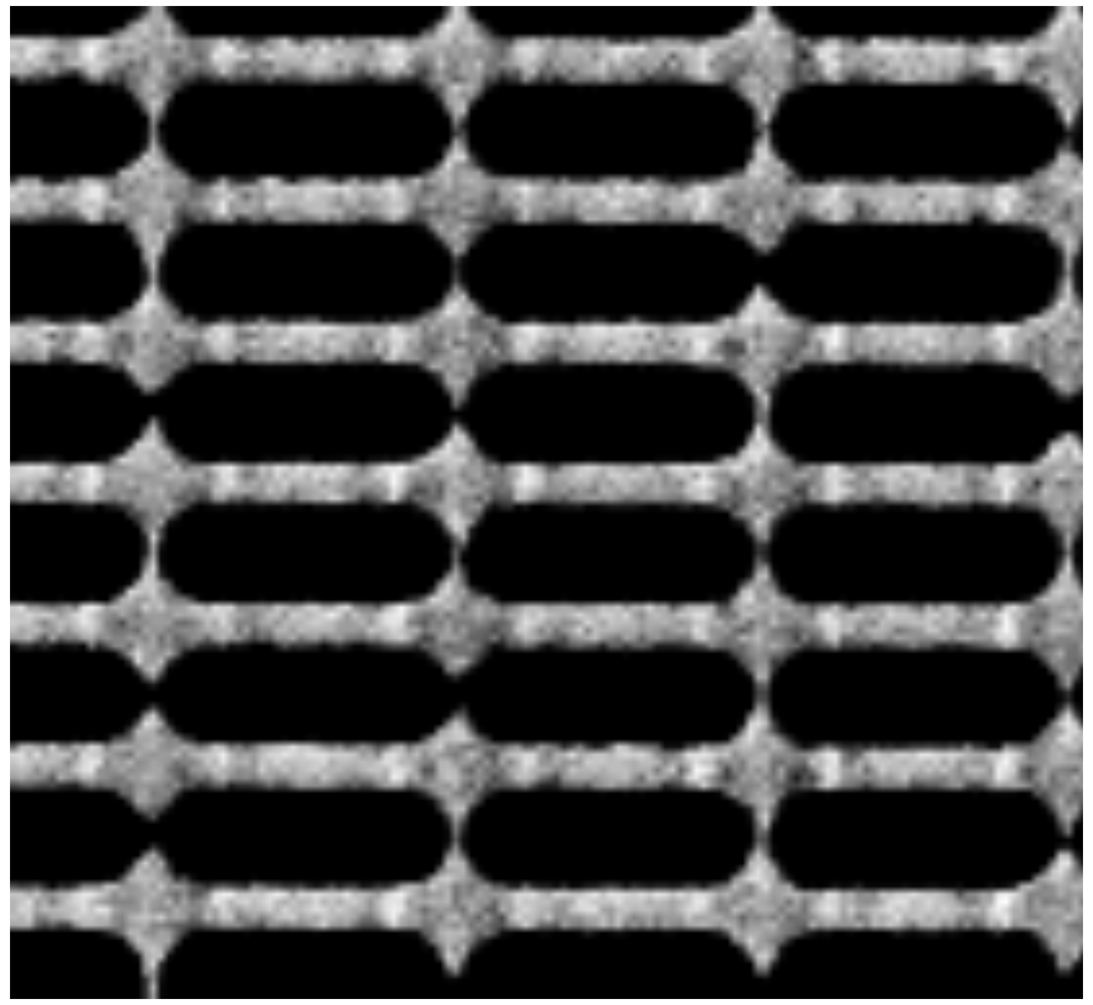
*GDS2 active layer example*



*Core GDS2 for FIB NAVIGATION*

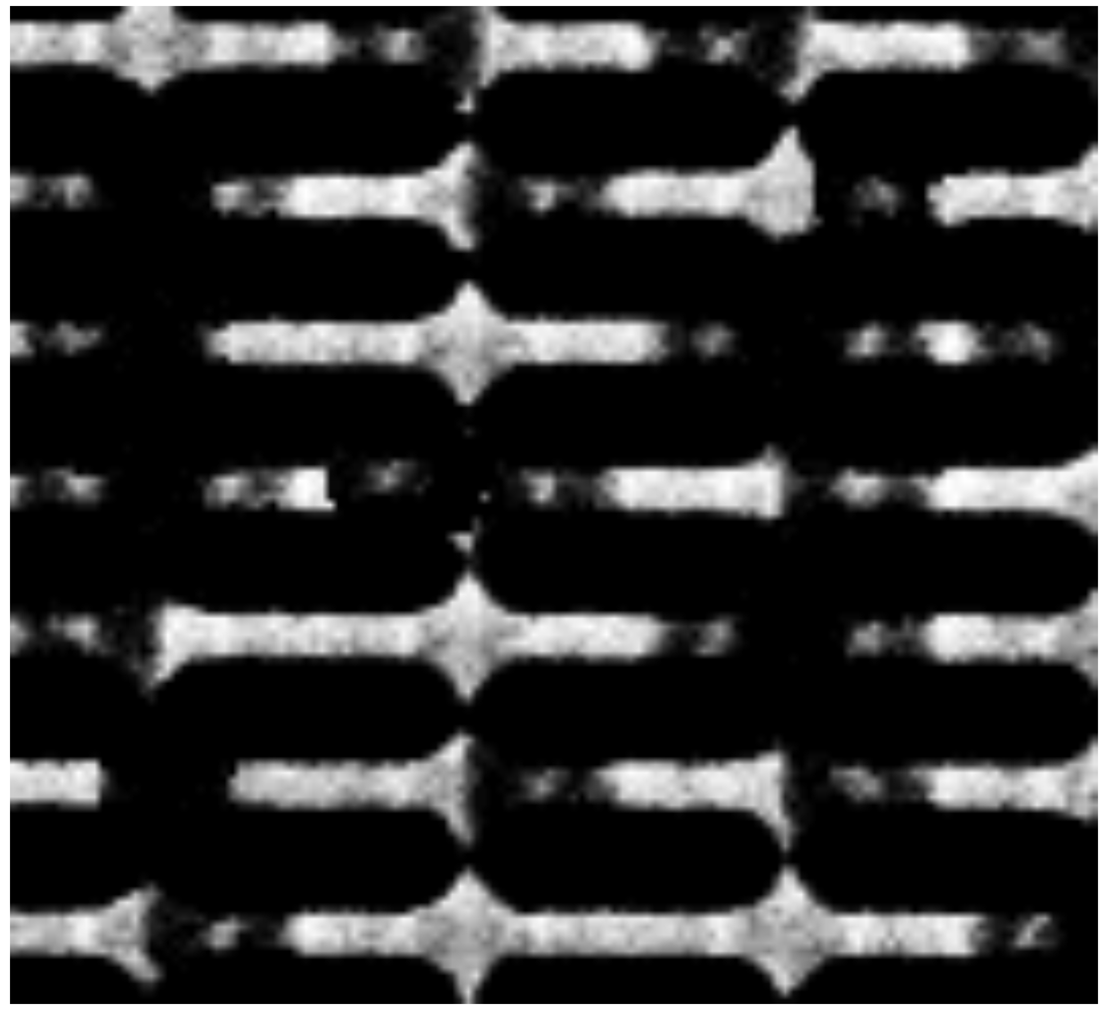
# Reading The ROM

- Getting the « raw » bits is feasible.
- Is the ROM encrypted?



*Bits before wet chemical dopant etch*

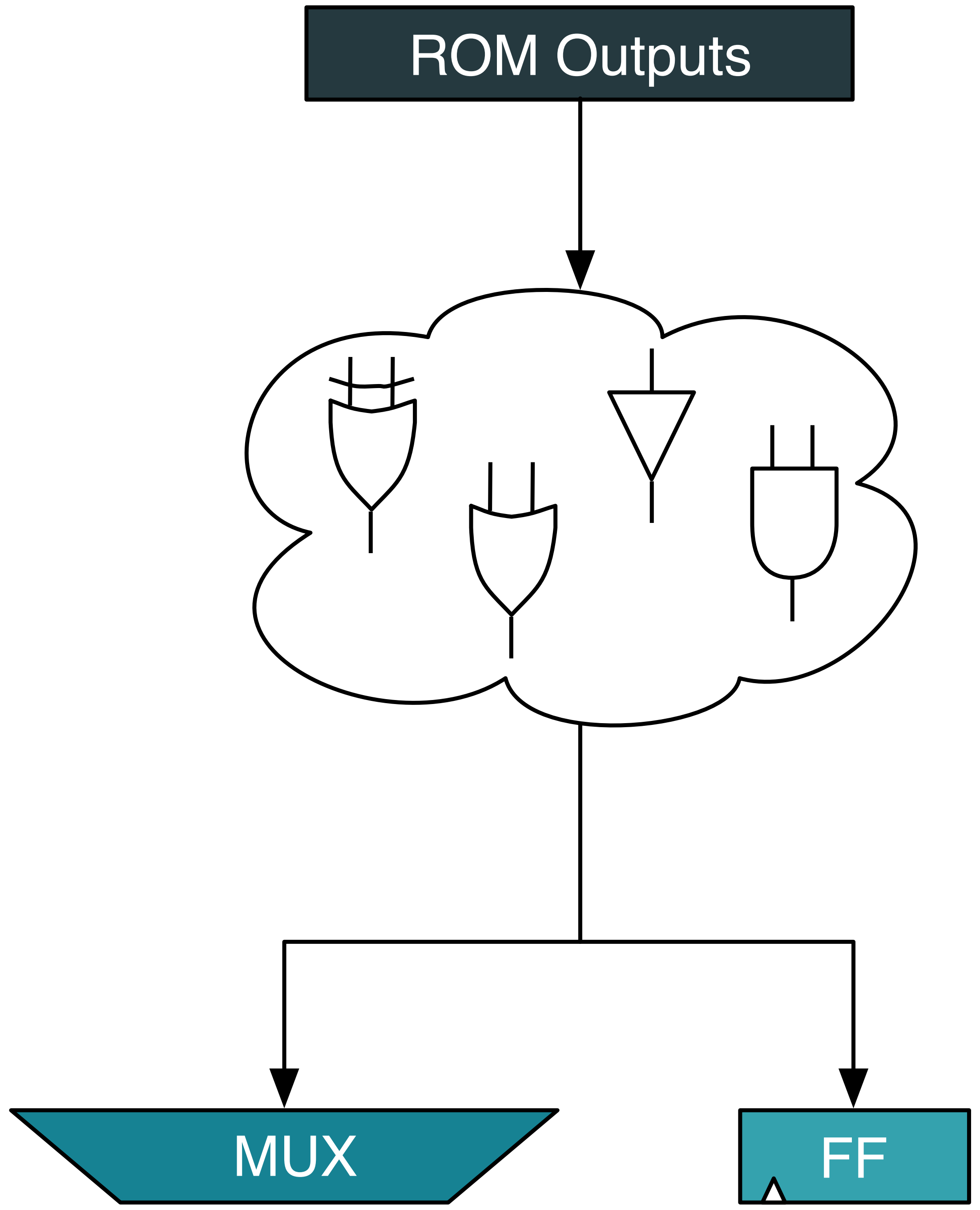
*Dopant etch*



*Bits revealed by etching*

# Reading The ROM

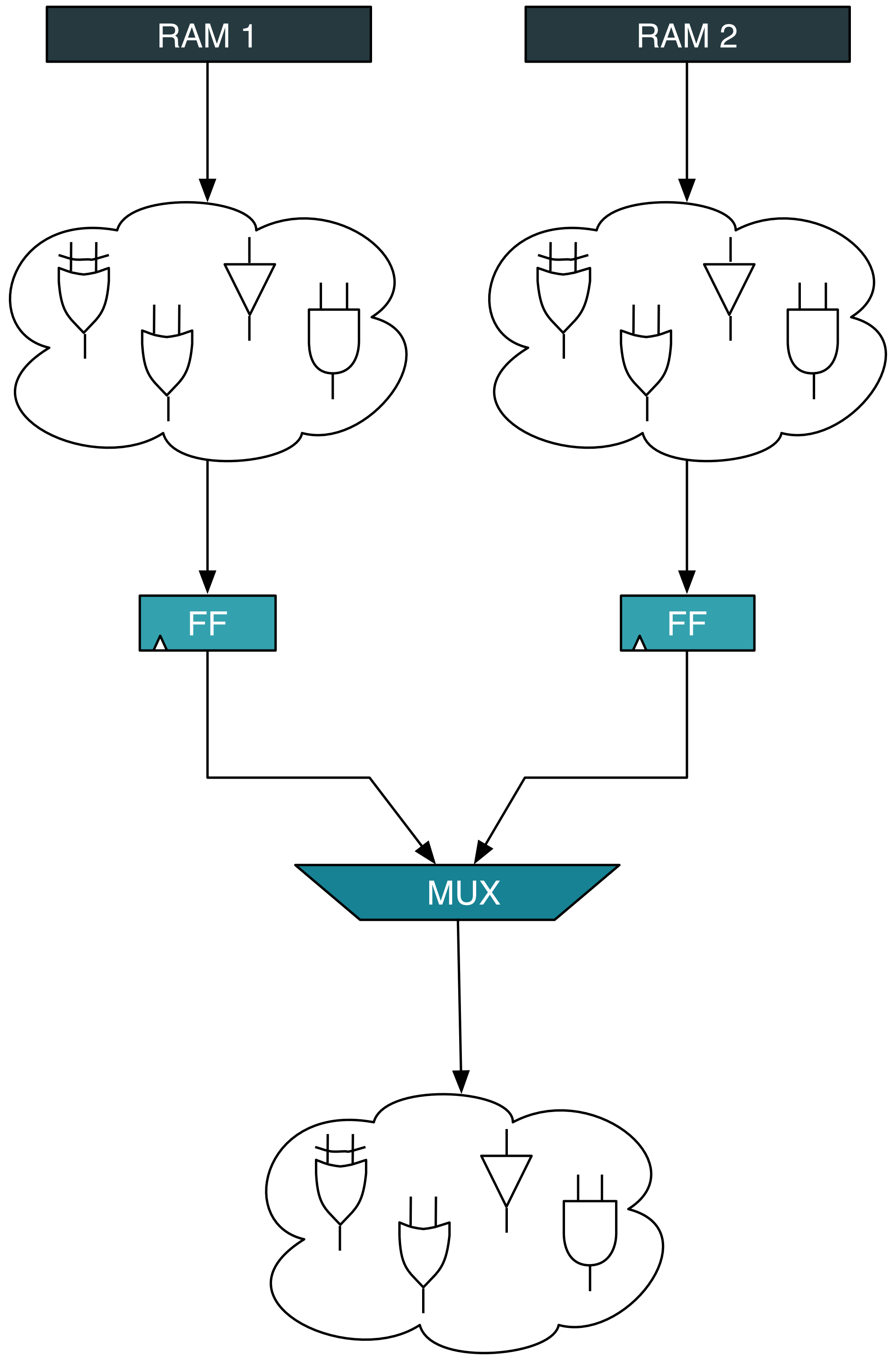
- ROM data bus goes to an encryption bloc
- Having Muxes and Flip-Flops on the same path may indicate that decryption operation can take several clk cycles.
- This path has not been completely reversed
- ROM can be read after studying the encryption without any Focused Ion Beam edit.



*ROM Data Path*

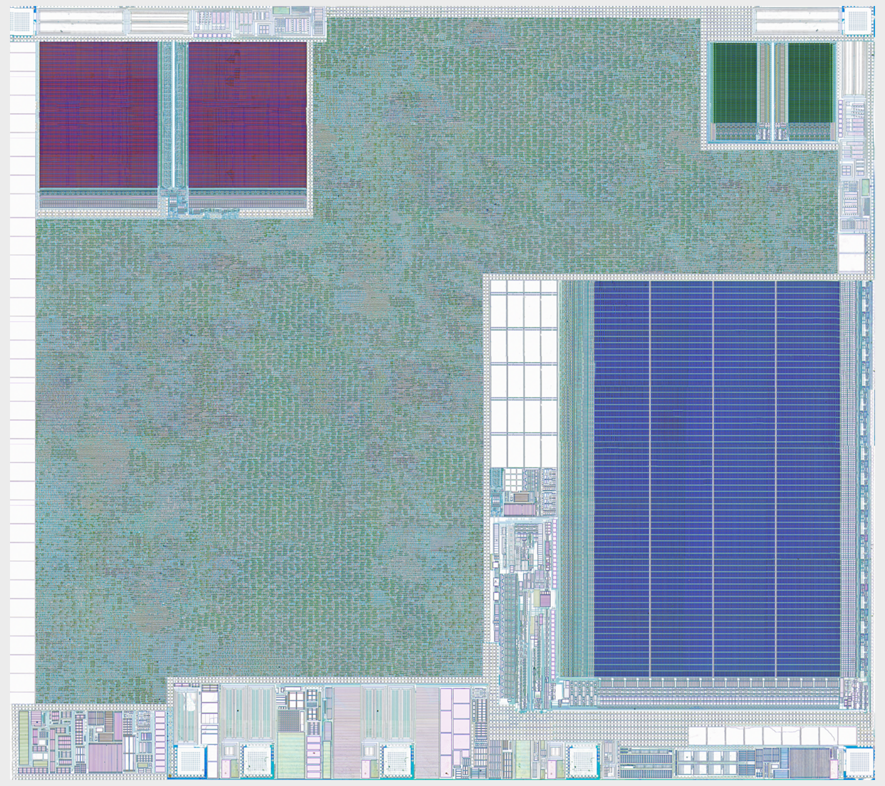
# 2 Blocs of RAM

- Both RAM are encrypted
- RAM and ROM are on the same clk domain
- Shared RAM with the crypto accelerator?



*RAMs Data Path*

# Overview

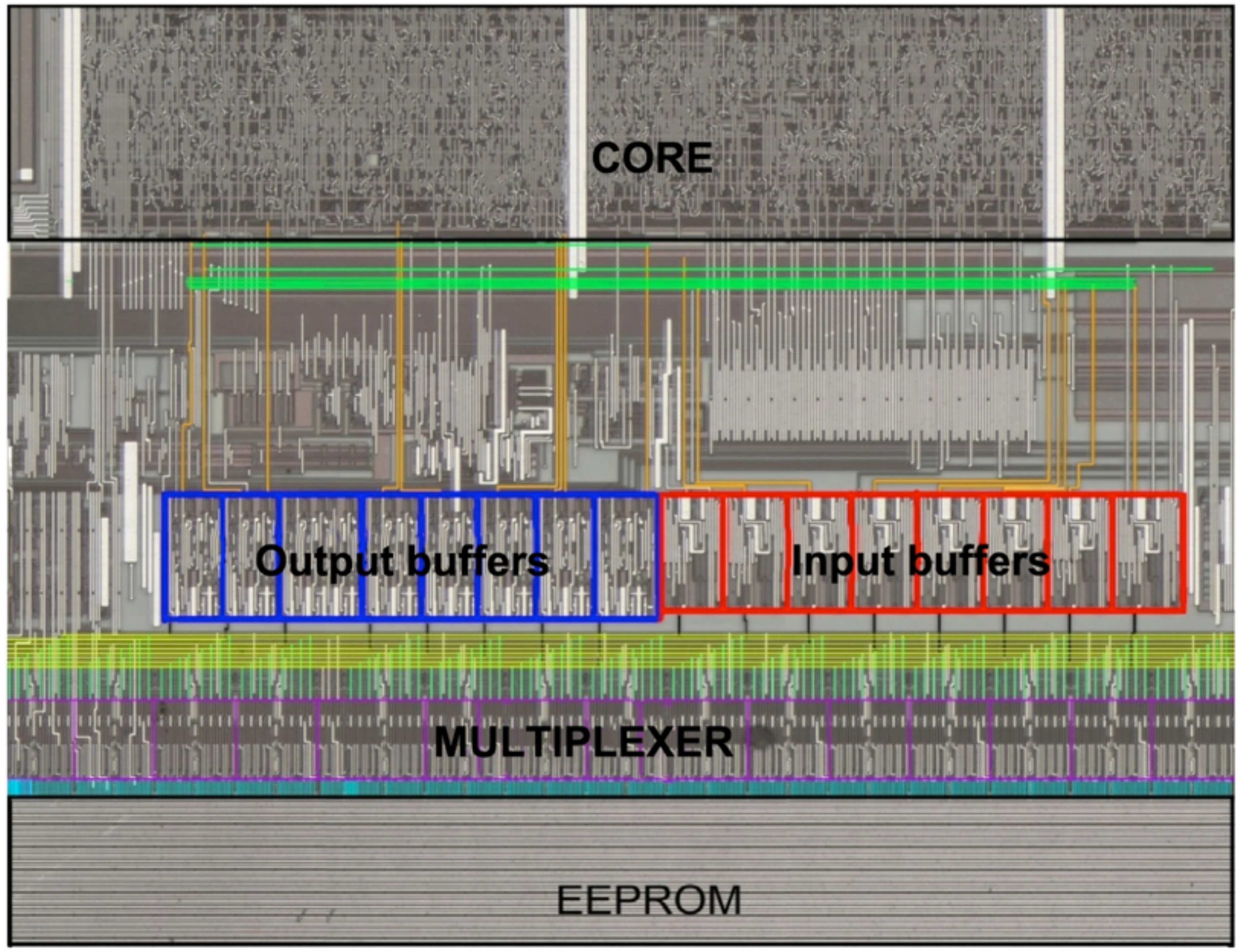


Conclusion

# Timing : generation benchmark

- The first Linear Code Extractions did not require expensive equipments such as FIB and SEM.
- The main memory was not scrambled neither encrypted.
- Buffers were easily accessible.

- Extracting such a chip would require very little effort nowadays.



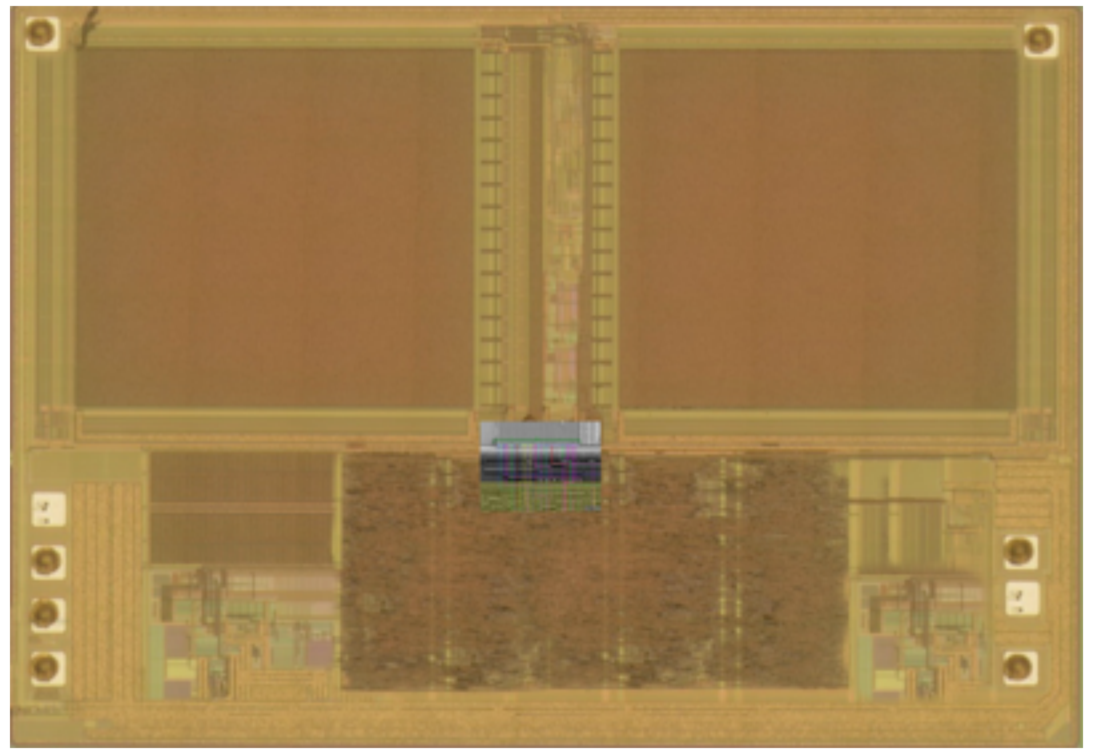
*Unprotected Bus*

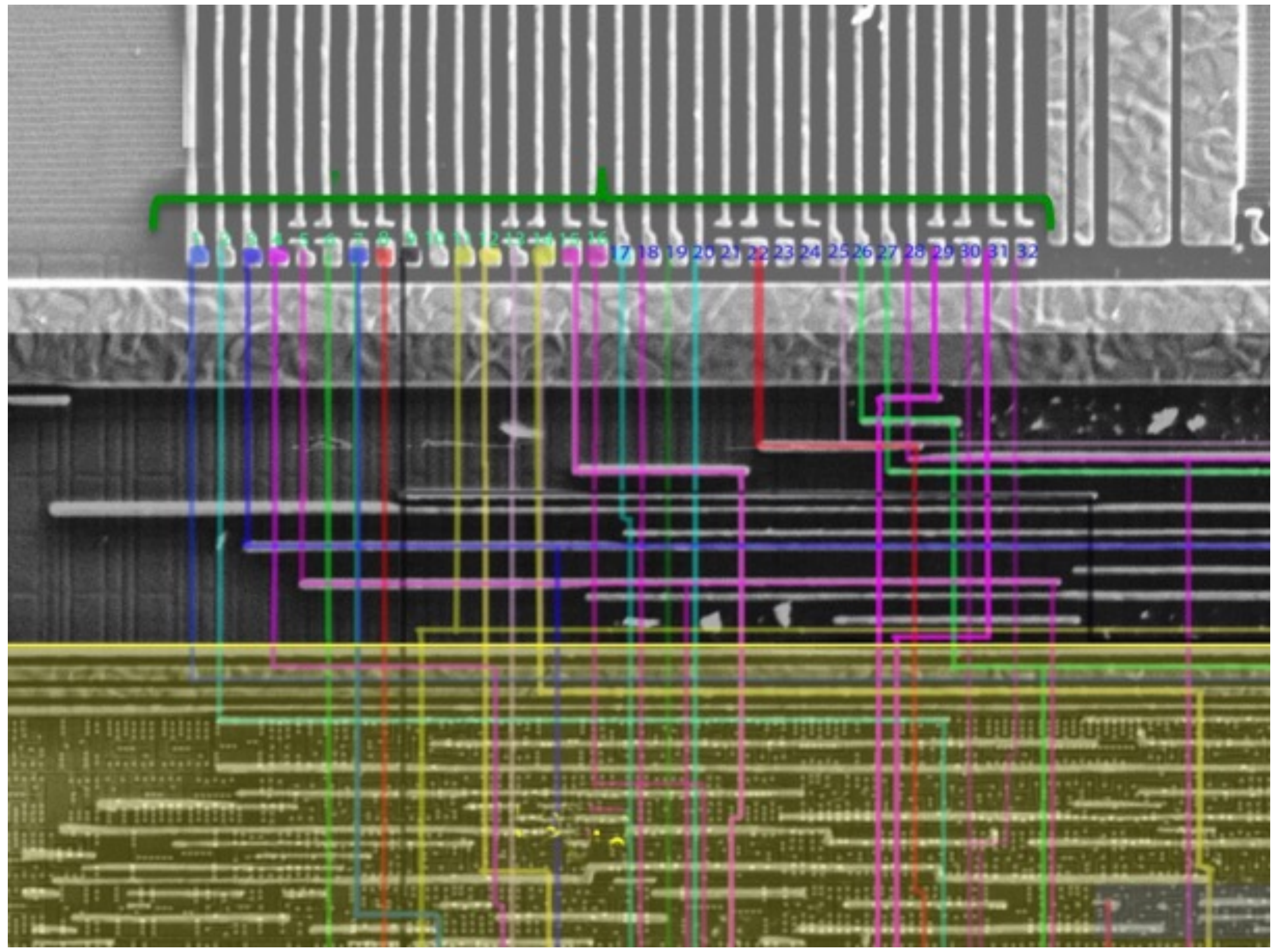
# Timing : generation benchmark

- To avoid easy access to the logic, multiplexers and buffers have been hidden inside the core.

## Scrambling

- 8 bits processor
- 32 bits FLASH output going to the core



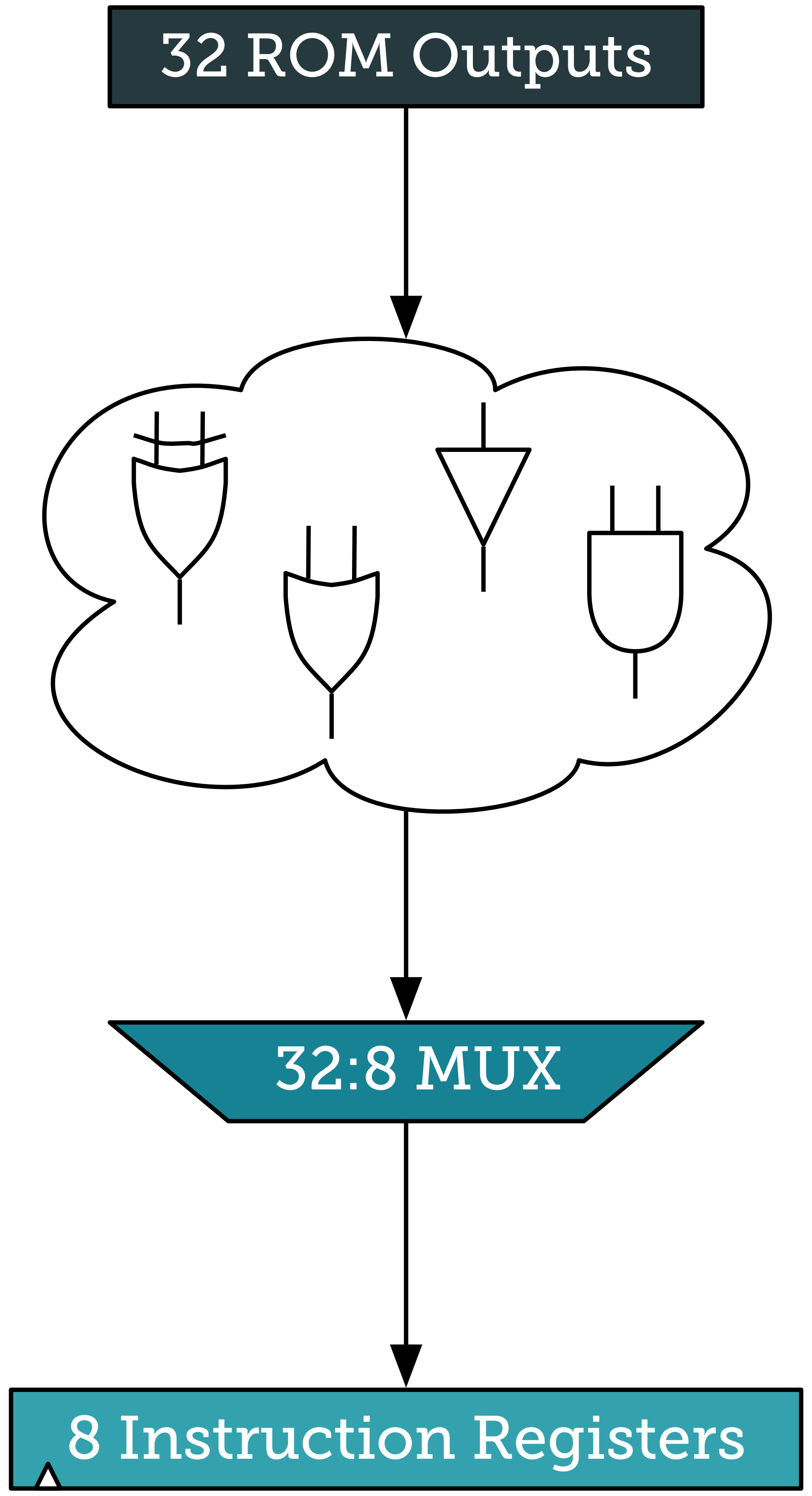


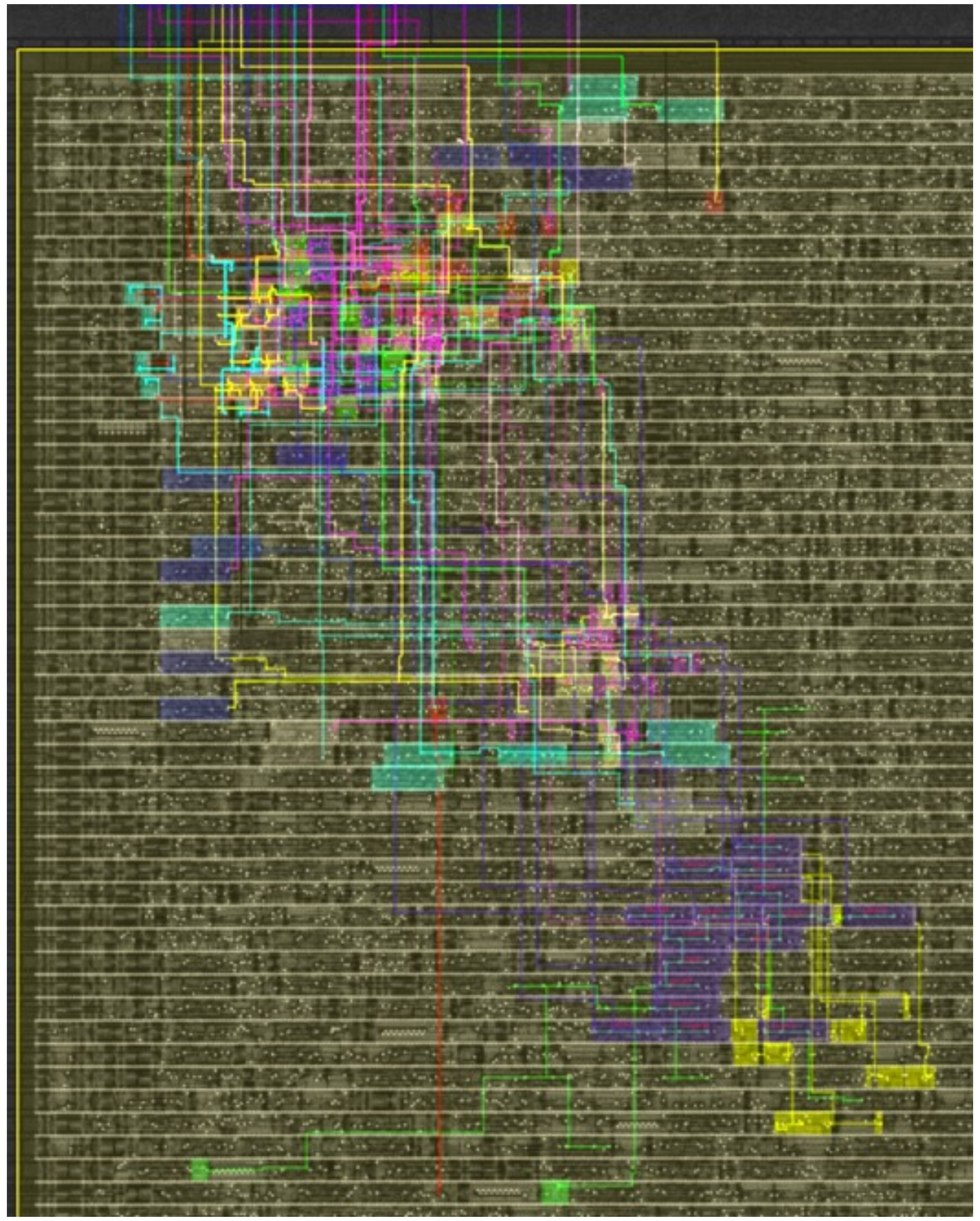
*Manual Tracing*

# Timing : generation benchmark

## Step by step

- Lines have to be traced inside the core
- The core contains a multiplexer for the 32-bit lines
- Identify the 8 output bits of the multiplexers



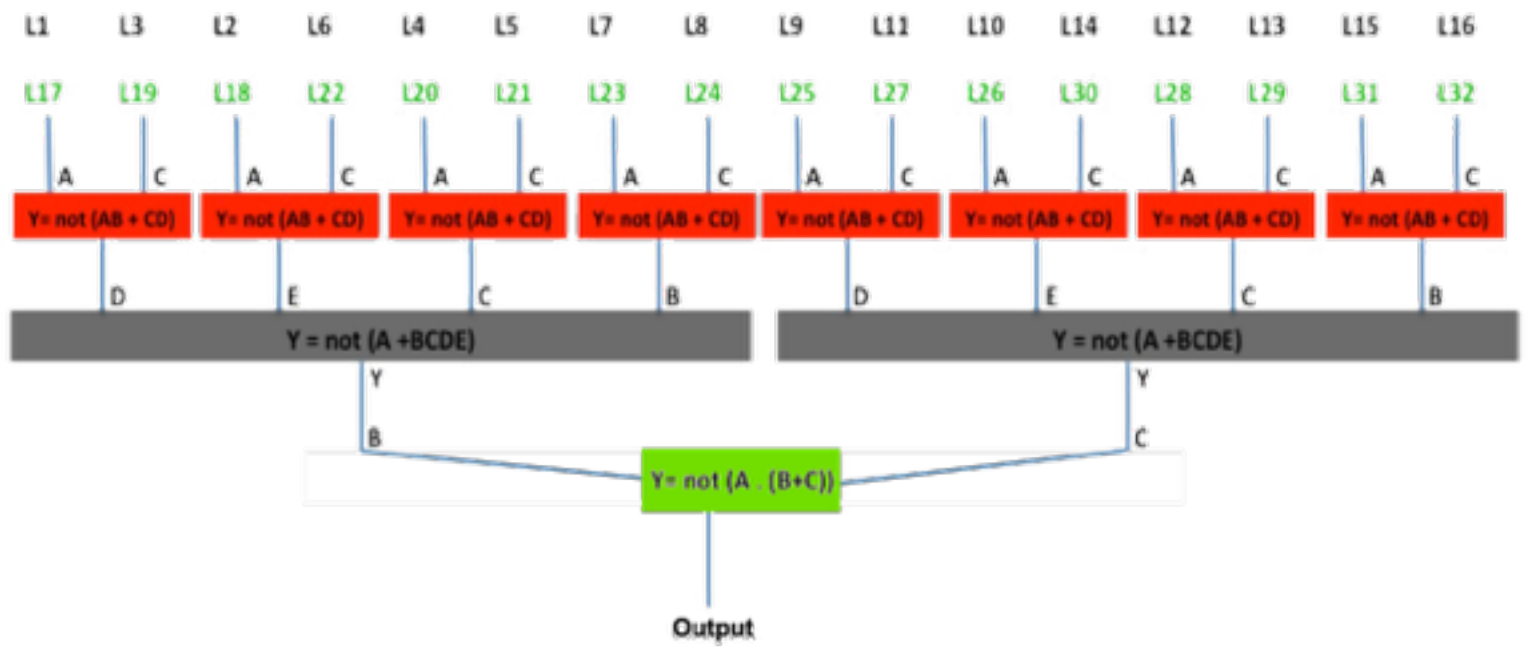


*Manual Tracing inside the core*

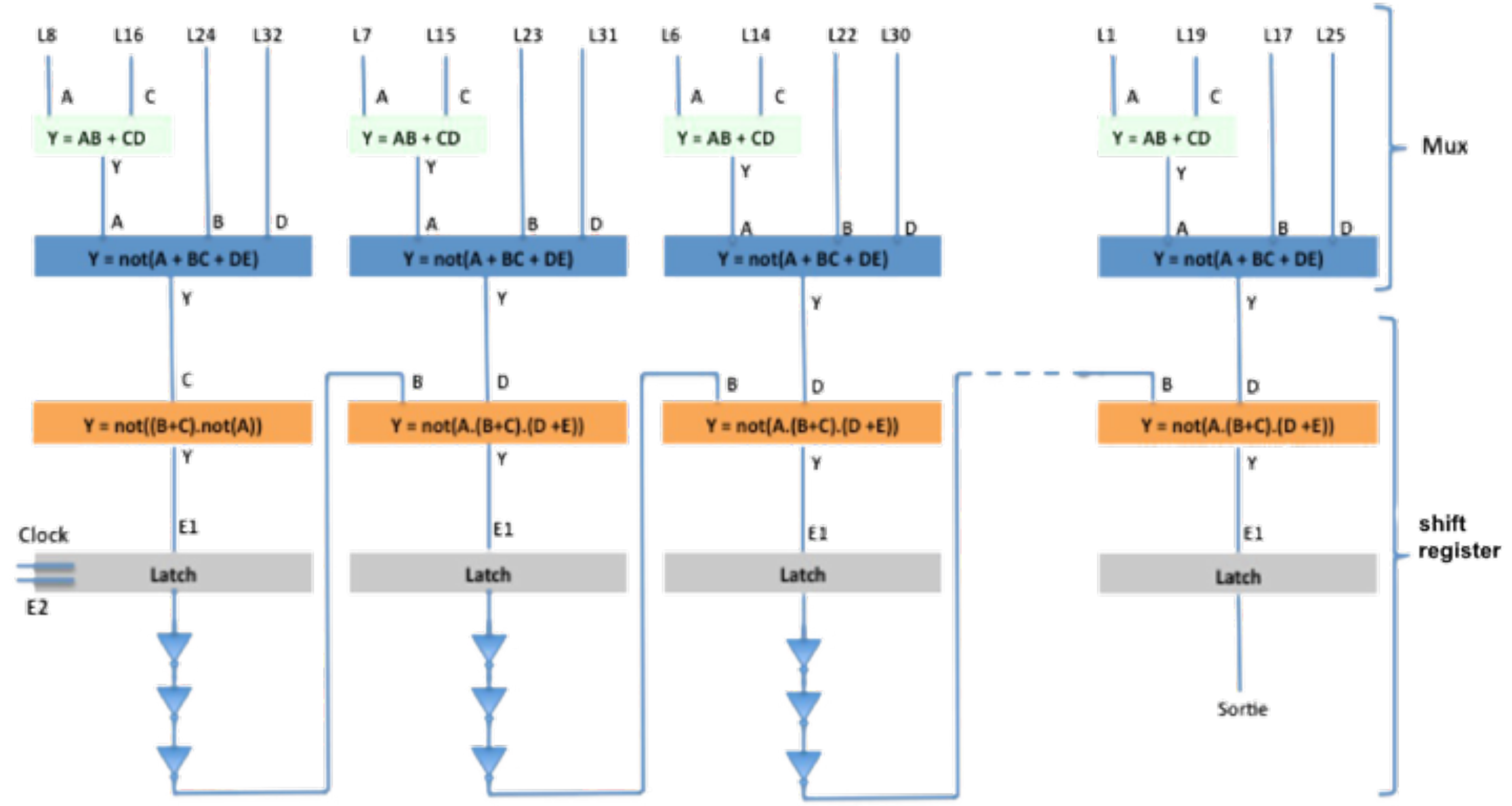
# Timing : generation benchmark

## Step by step

- 3 paths can be followed
- 2 of them can not be exploited



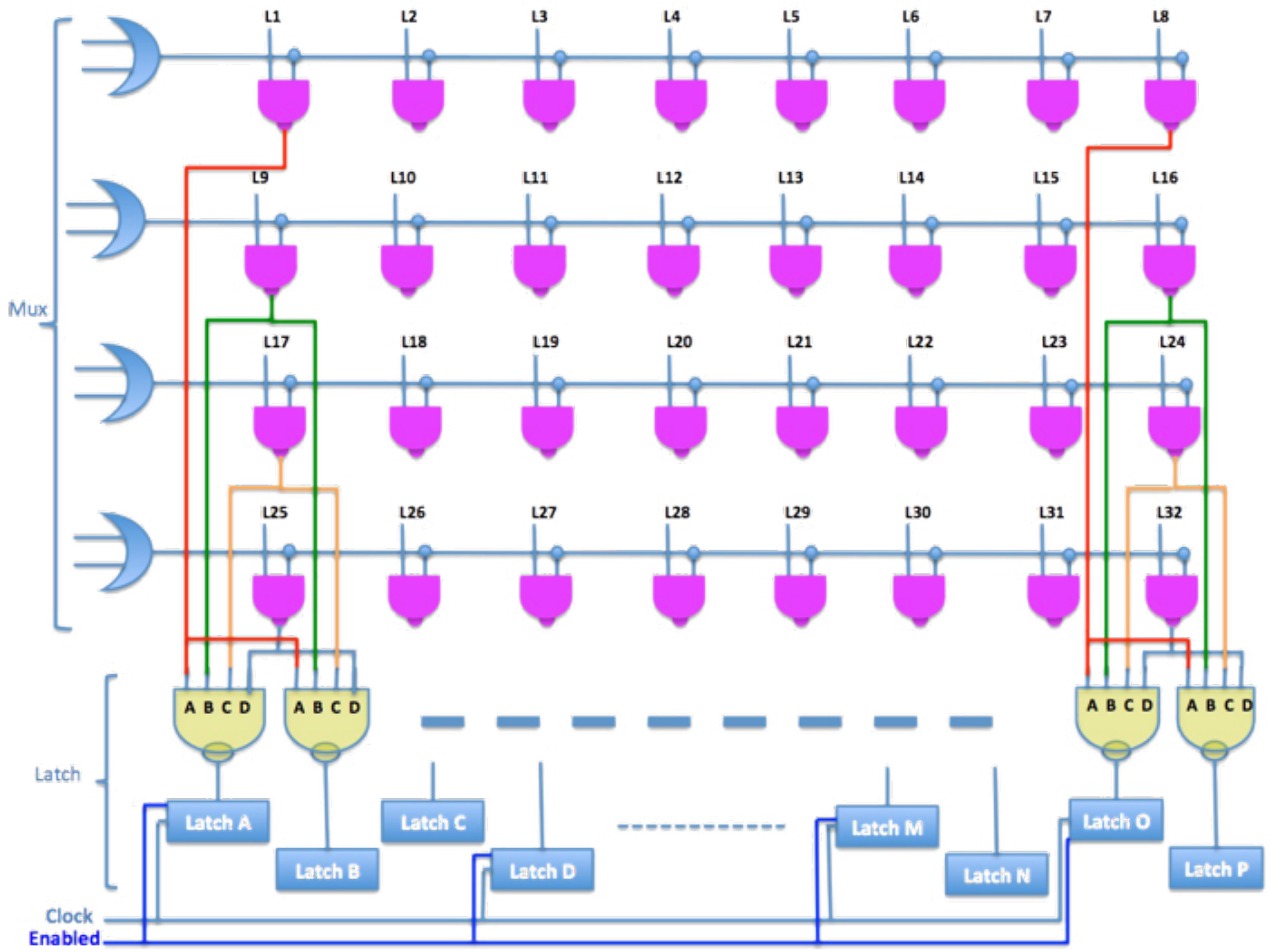
L1 L3 L2 L6 L4 L5 L7 L8 L9 L11 L10 L14 L12 L13 L15 L16
L17 L19 L18 L22 L20 L21 L23 L24 L25 L27 L26 L30 L28 L29 L31 L32
A C
Y= not (AB + CD)
D E C B
Y = not (A +BCDE)
Y
B C
Y= not (A . (B+C))
Output



# Timing : generation benchmark

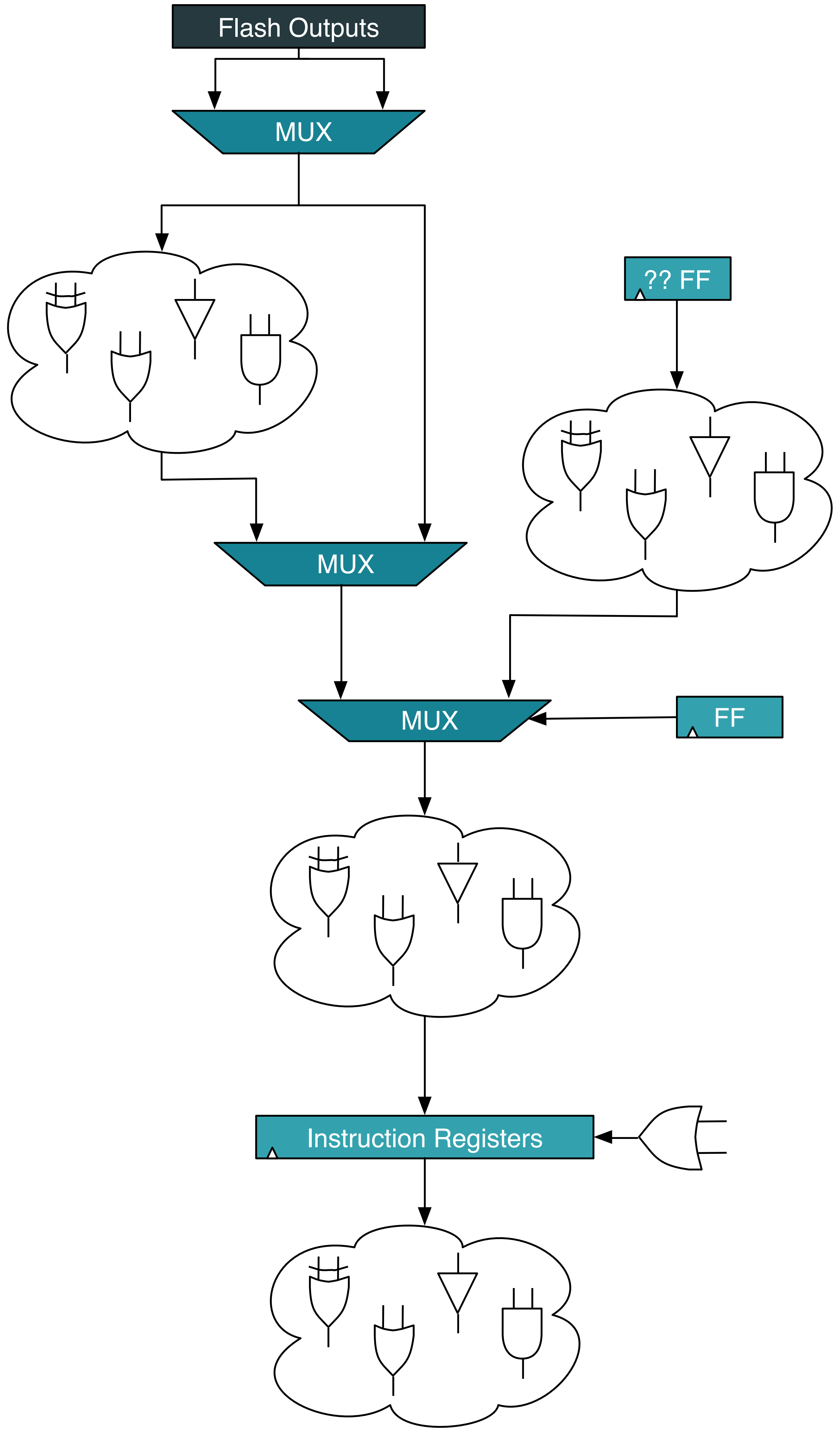
## Step by step

- Multiplexers were hidden
- Data was not encrypted
- Finding the correct spot took some time : ~ 2 months.



# Timing : generation benchmark

- New methodology is already successful
- Time of this particular study is short
    - Deprocessing and imagery can be performed in less than 2 weeks.
    - Interconnects are extracted and the result checked in another 2 weeks.
    - The tools used for that study were in a mode used when picture quality is low or when feature extraction has not been verified.
    - Standard Cell Library has been extracted while tracing signals, leading to 22.000 extracted instances inside the core.
    - Tracing RAM, ROM and Flash to the Instruction Register and verifying its location with an overview of the Instruction decoder took 1,5 week.



*Flash bus schematic*

# Conclusion

- The target IC has the characteristics of a secure chip.
  - Shield
  - Internal Oscillator
  - Memory encryption
  - Obfuscation of the different parts inside a single core
  - …
- Linear Code Extraction would be the best method to read the main memory
- ROM could be read by a deep Hardware Reverse Engineering

# Conclusion

- Time necessary to perform the study was 2 weeks of feature extraction related work and an extra week and a half to find where and how to perform a Linear Code Extraction.

- This methods speeds up the regular process by a significant factor.
- It also opens doors for semi-invasive attacks where the position of important standard cells could be used to narrow down one study.
- Hardware custom implementation are questionable.

# CONTACT

## Olivier Thomas

Chief Executive Officer
+33 6 64 80 06 87
olivier@texplained.com

## Clarisse Ginet

Head of Business Development
+33 6 35 54 12 04
clarisse@texplained.com

www.texplained.com