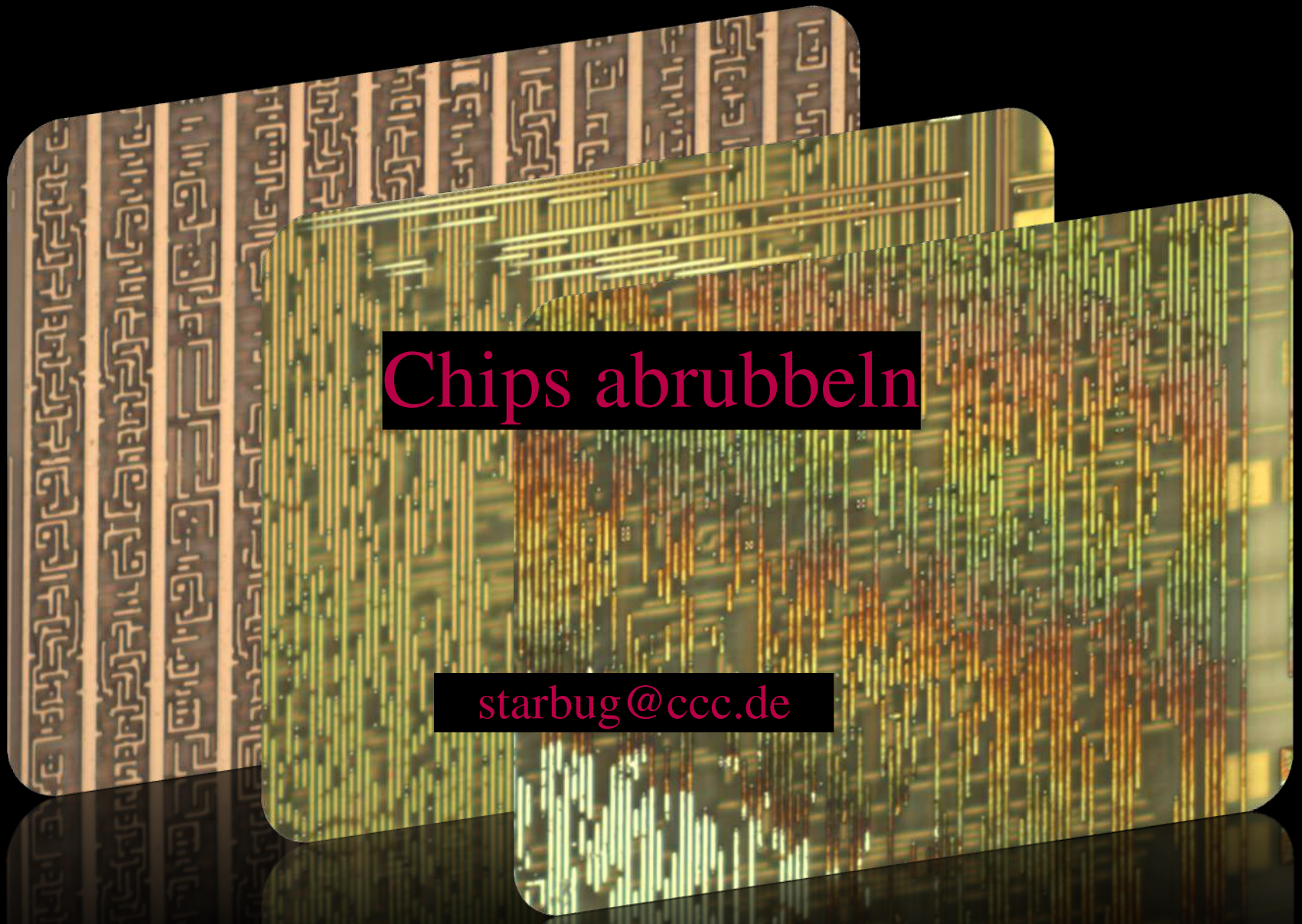
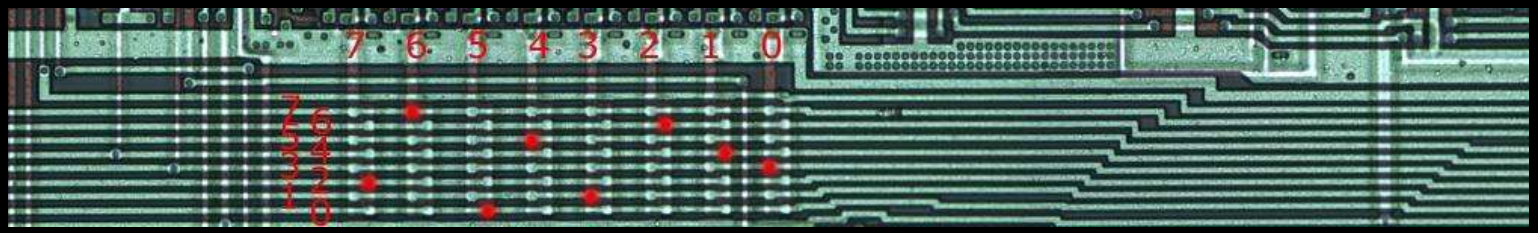

Chips abrubbeln
starbug@ccc.de

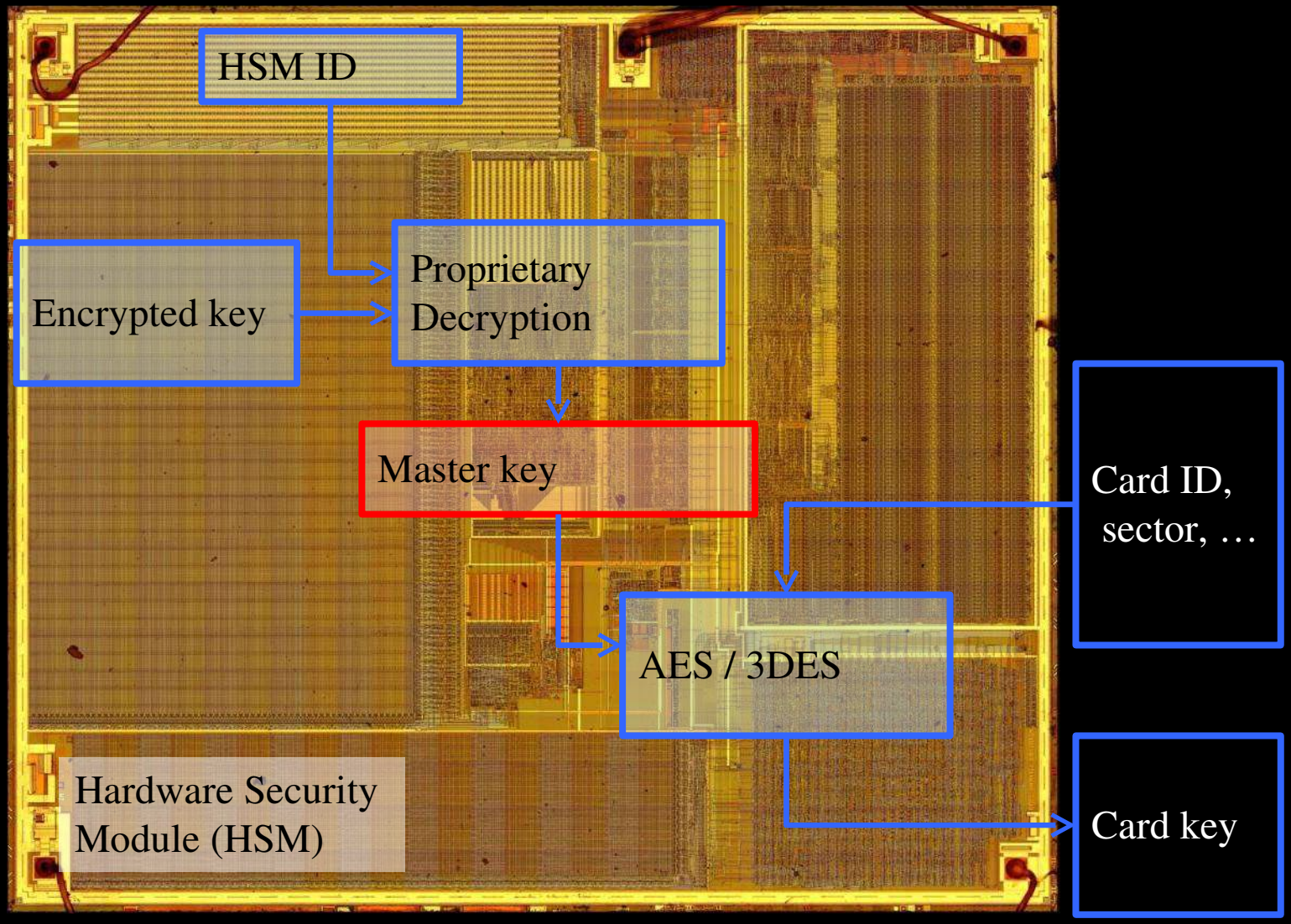
Wieso?

- Aufbau von Microchips
  - Position von Fuses (unter Coverlayern)
  - Busscrambling

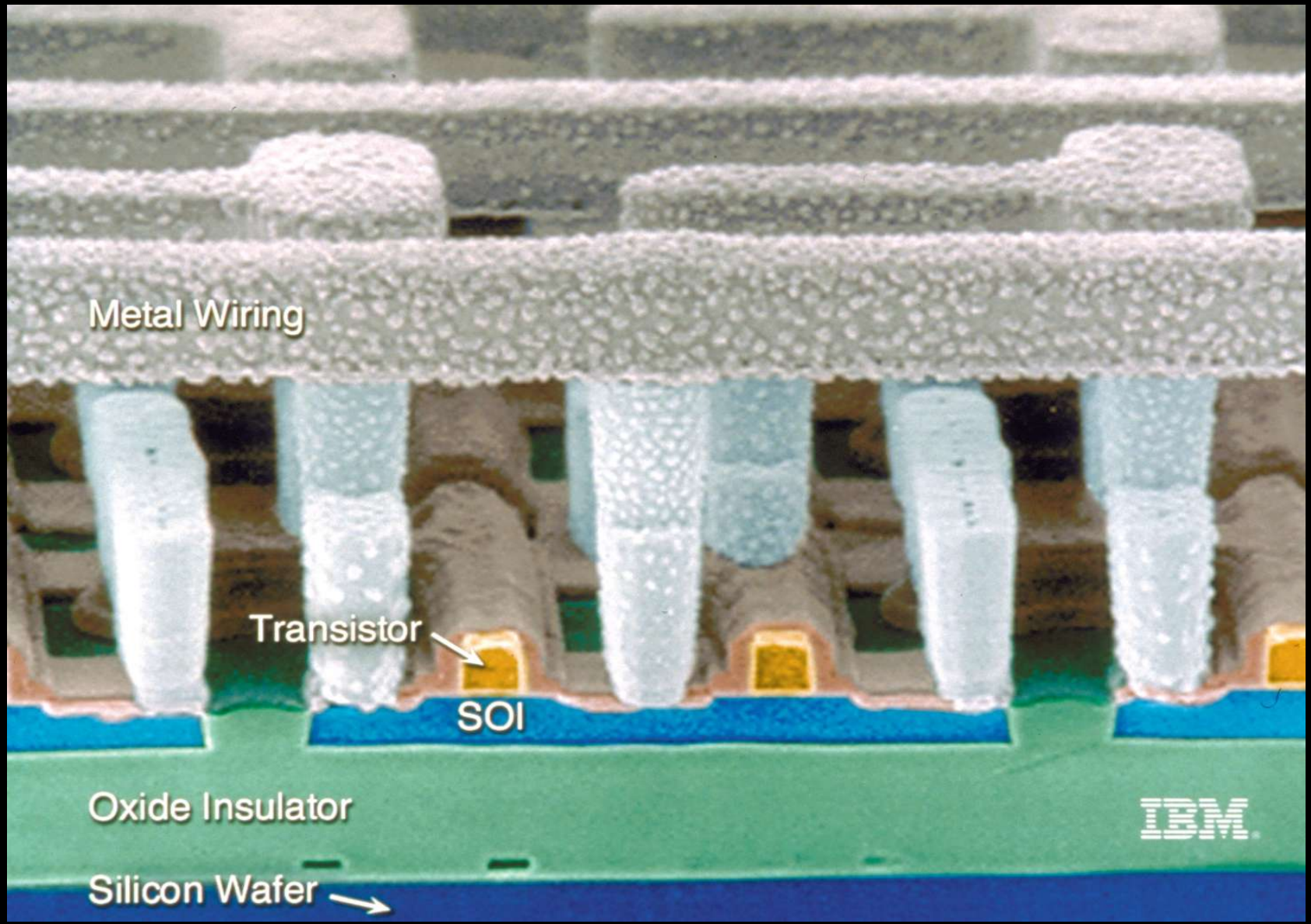


- reverse engineeren propritärer Kryptoalorithmen
  - Mifare classic (Crypto1)
  - Legic prime
  - DECT (DSC)
  - Hardware Security Modules (Geldautomaten)

Hardware Security Module



Aufbau eines CMOS-Chips



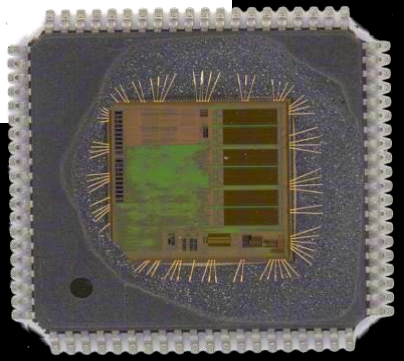
Extrahieren des Chips

Extrahieren des Chips aus dem Kartenkörpers

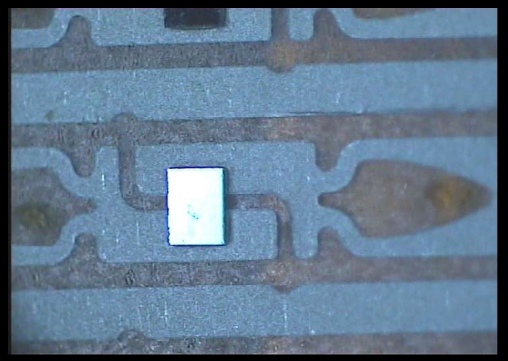
- Azeton

Entkapseln des Chips

- Rauchende Salpetersäure
- Kolofonium



Blanke Chips

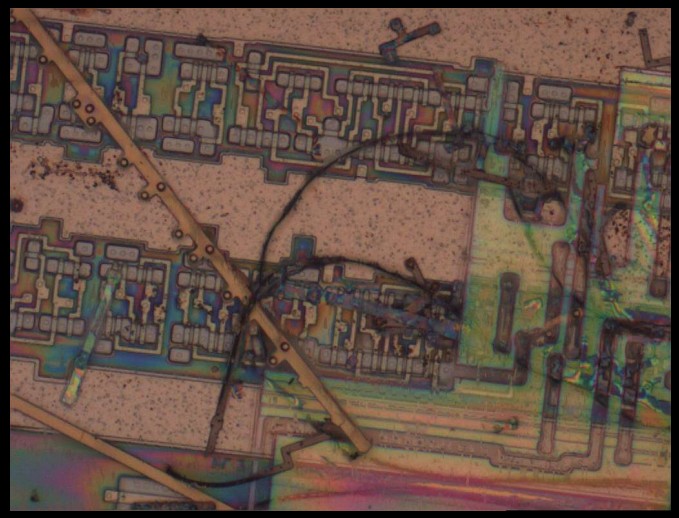


Schichtweises Abtragen

Ätzen mit Flußsäure
- für Transistorlayer

Plasmaätzen, FIB
- geringe Abtragsrate

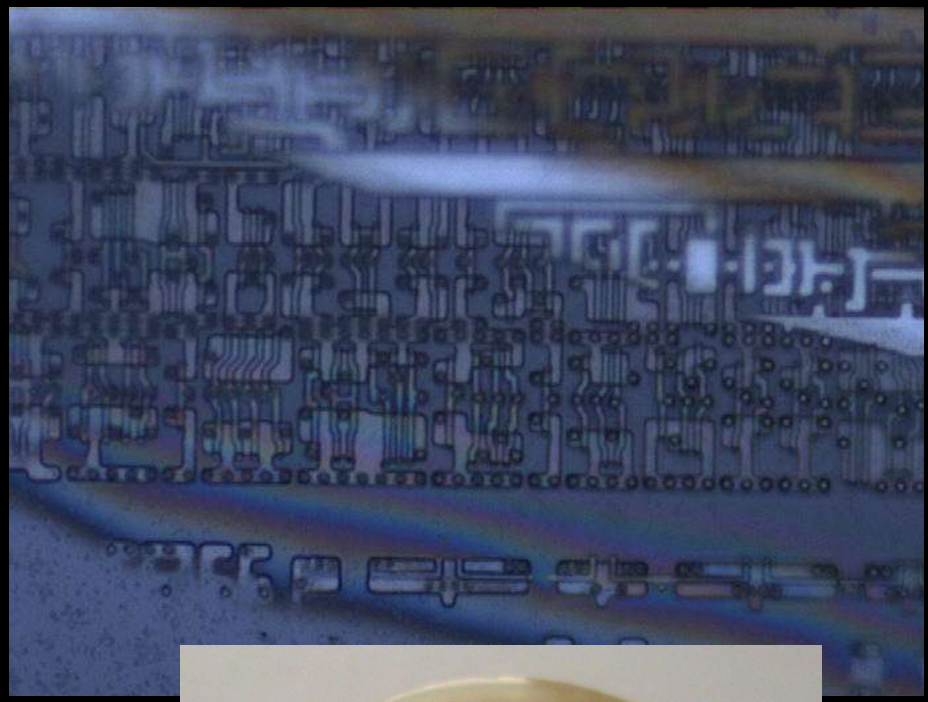
Polieren
- manuell
- automatisch



Paralleles Polieren

Eingießen des Chips
- Verkippung durch Bondpads

rückseitiges Aufkleben
- sehr plane Oberfläche
- parallel zu aktiven Layern



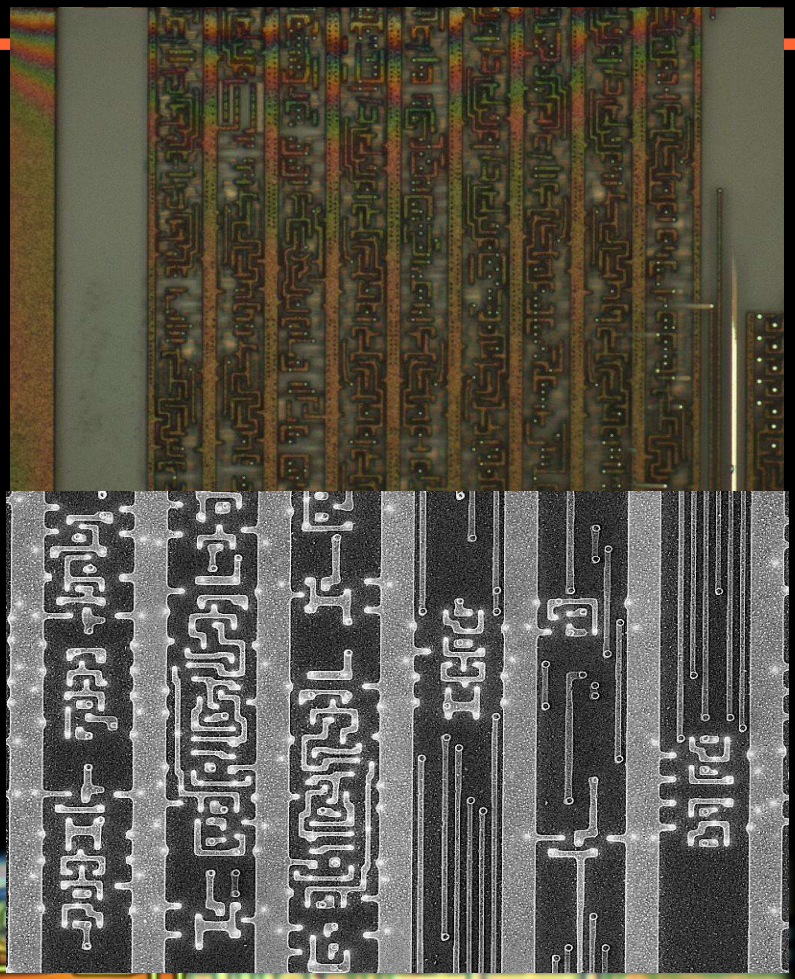
Bilder

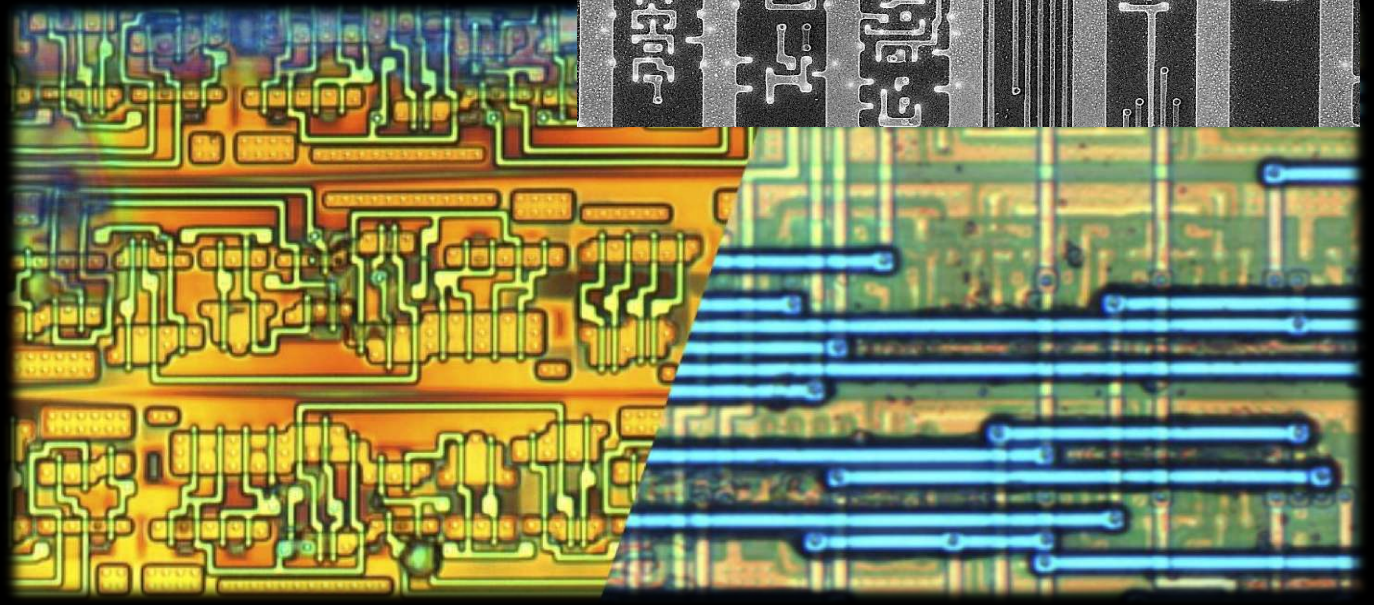
optisches Mikroskop
500 fache Vergrößerung
Kamera 1 Megapixel

konfokales Mikroskop

REM

FIB



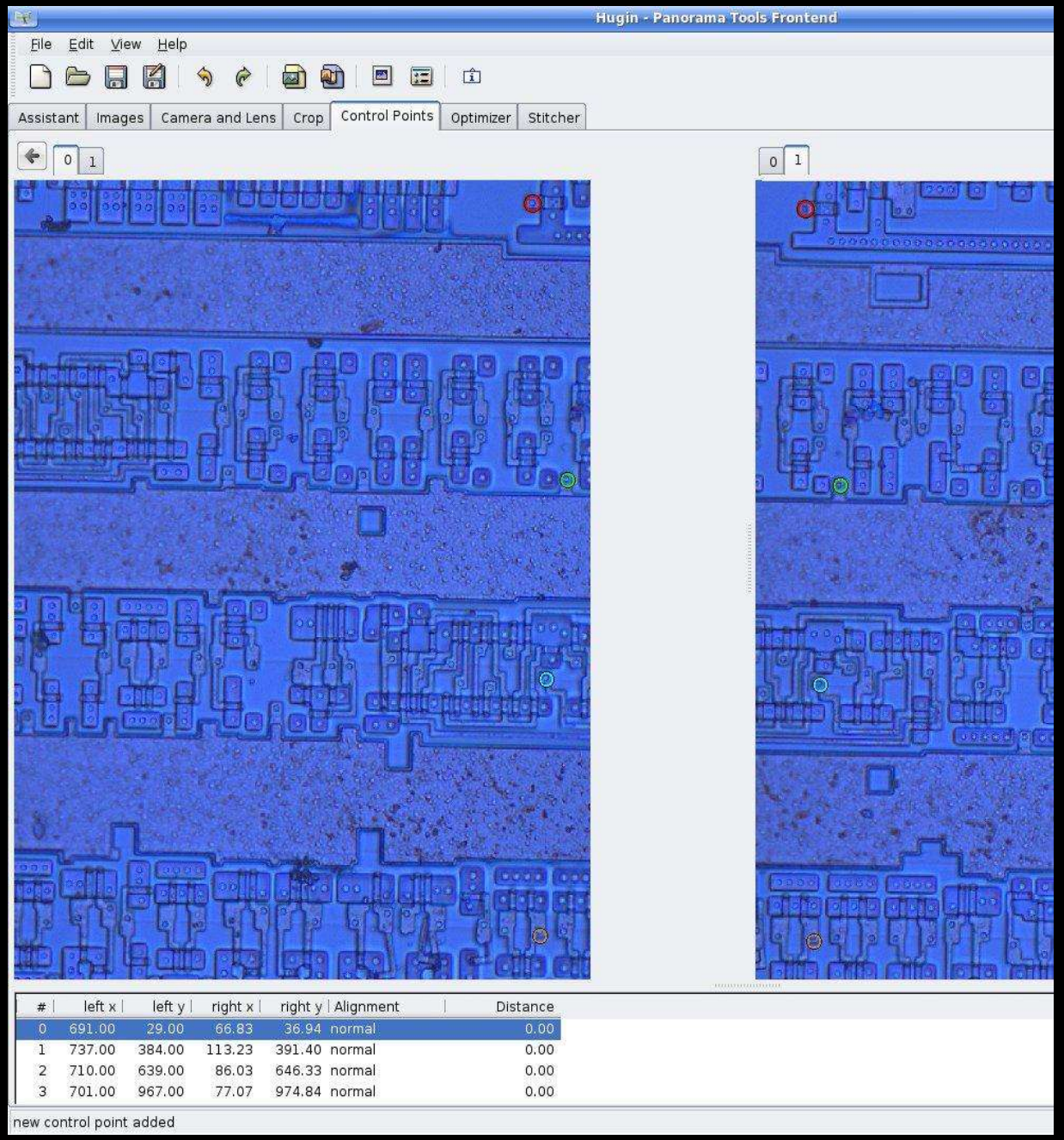


Stitching

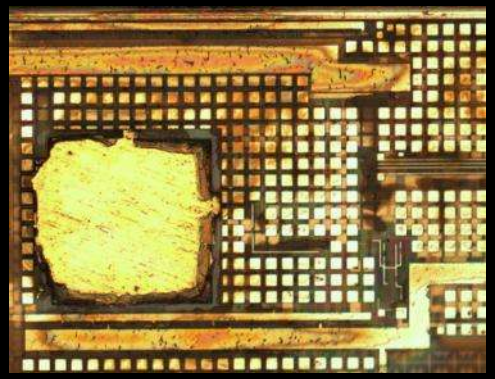
Zusammenfügen der Einzelbilder
(ca. 100 x 100 um)

Panoramasoftware

Ausrichten der einzelnen Layer

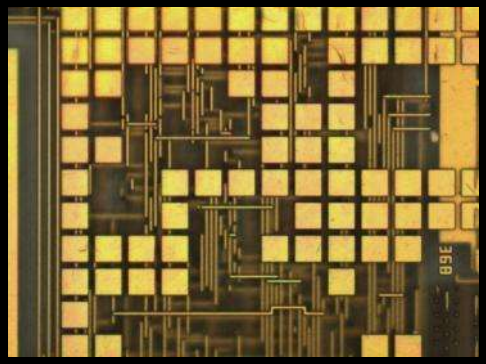


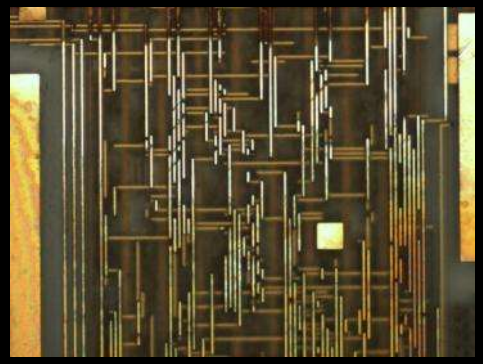
Mifare Classic

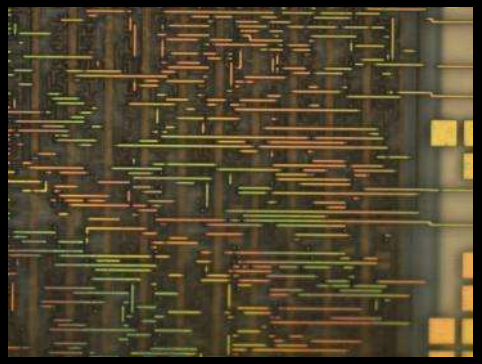


Cover layer

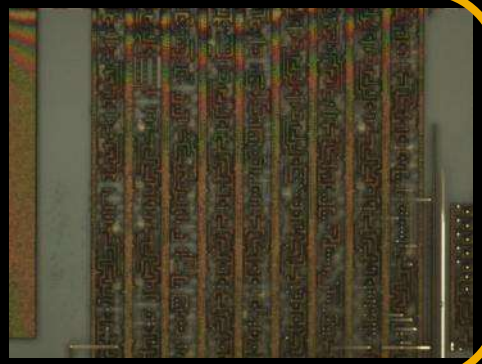
3 Interconnection layer

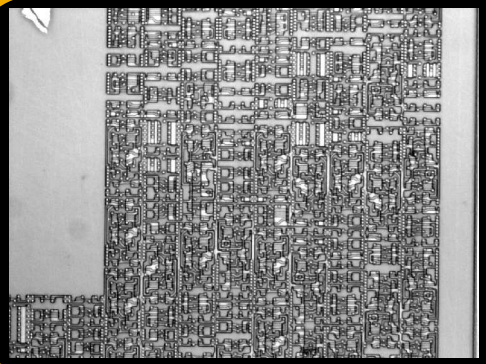






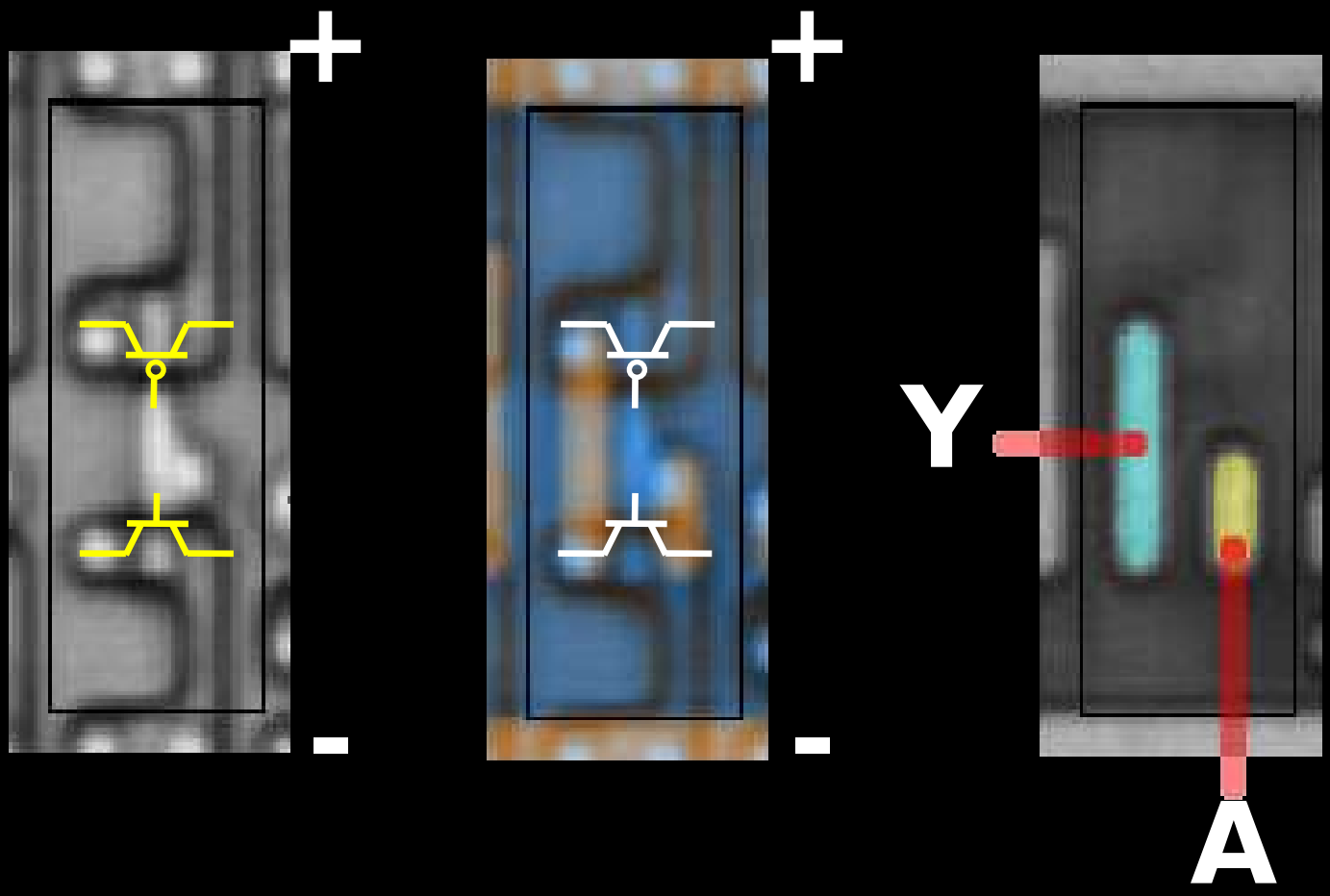
Logic layer



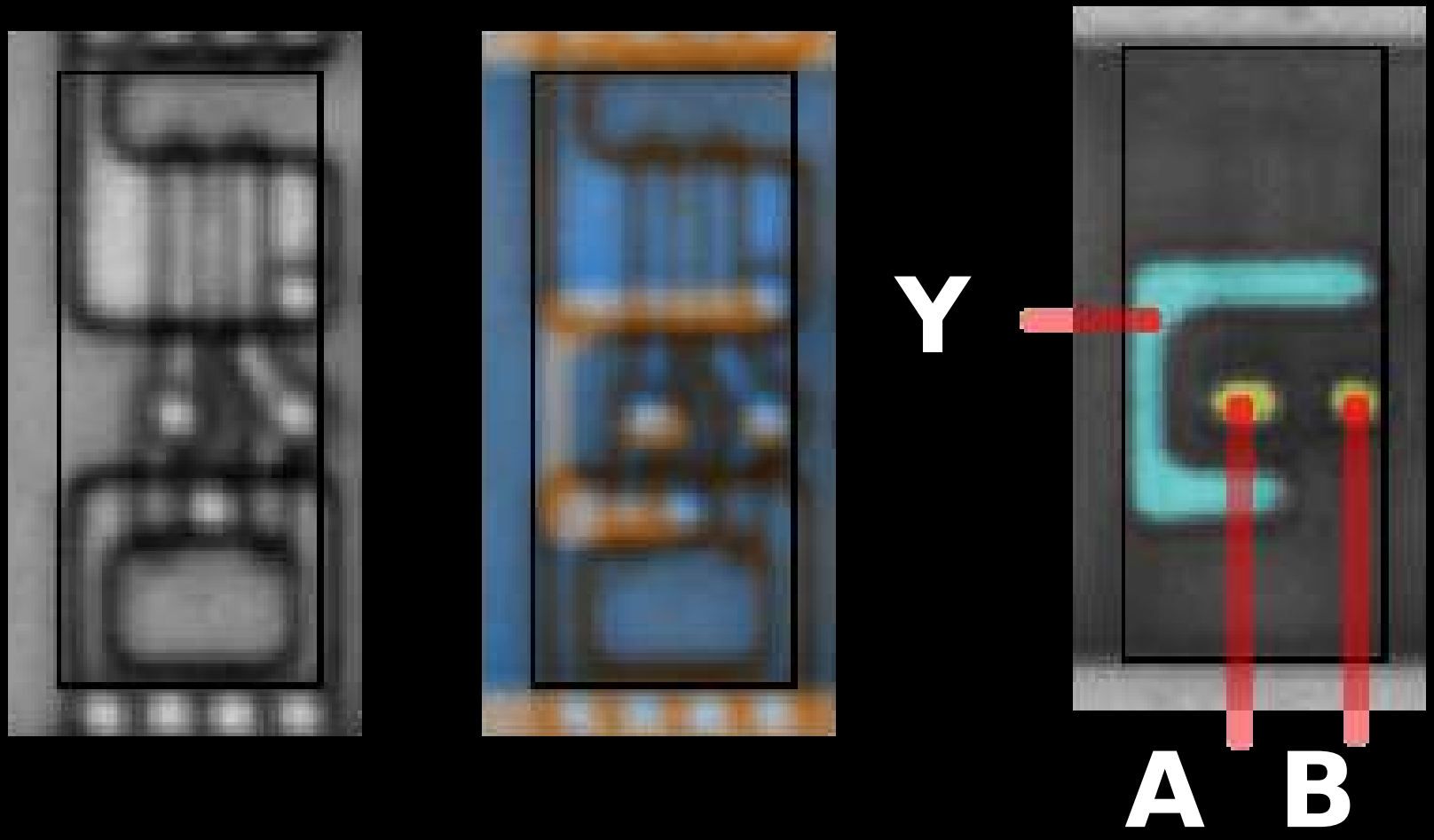


Transistor layer

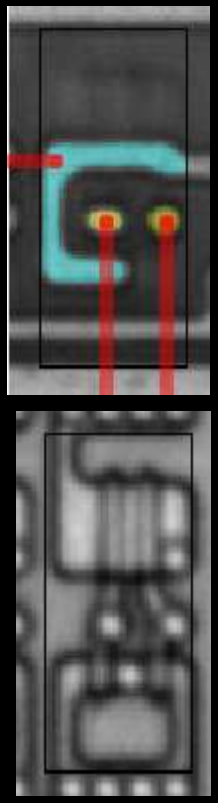
CMOS :: Inverter



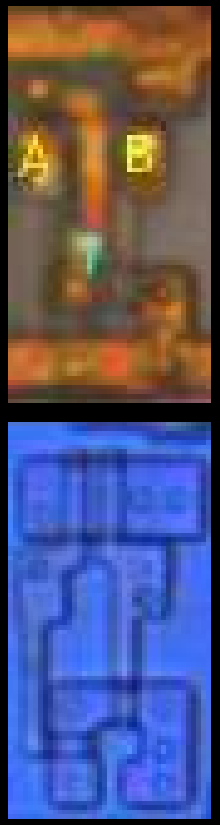
CMOS :: ??? (wer weiss es?)



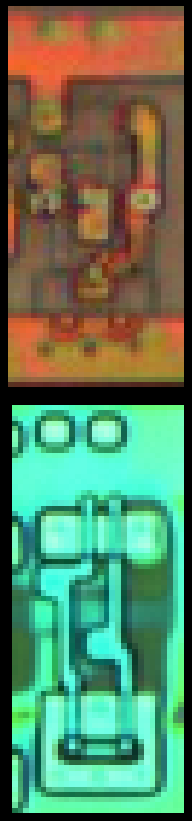
Siliconzoo.org :: 2-NOR



Mifare

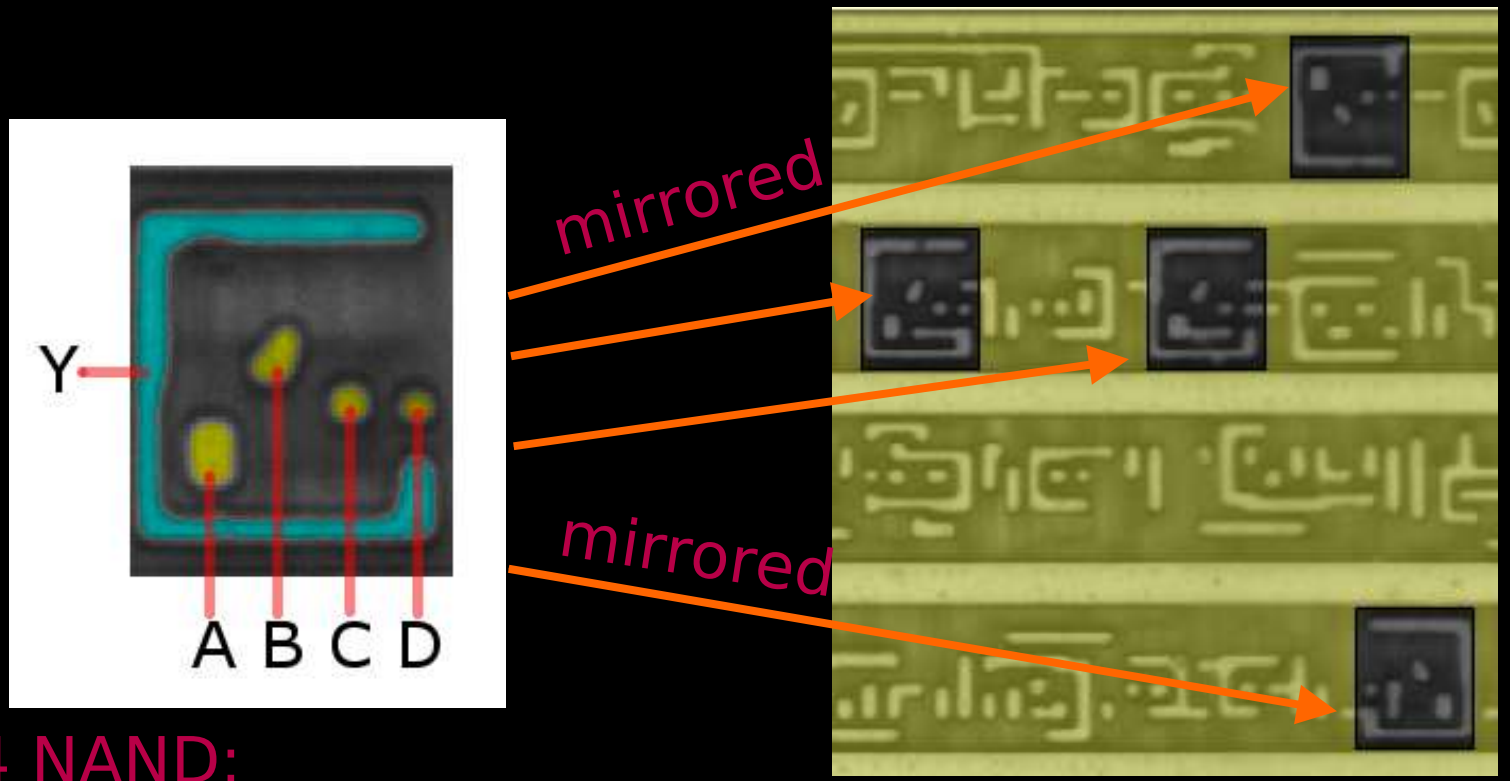


Legic



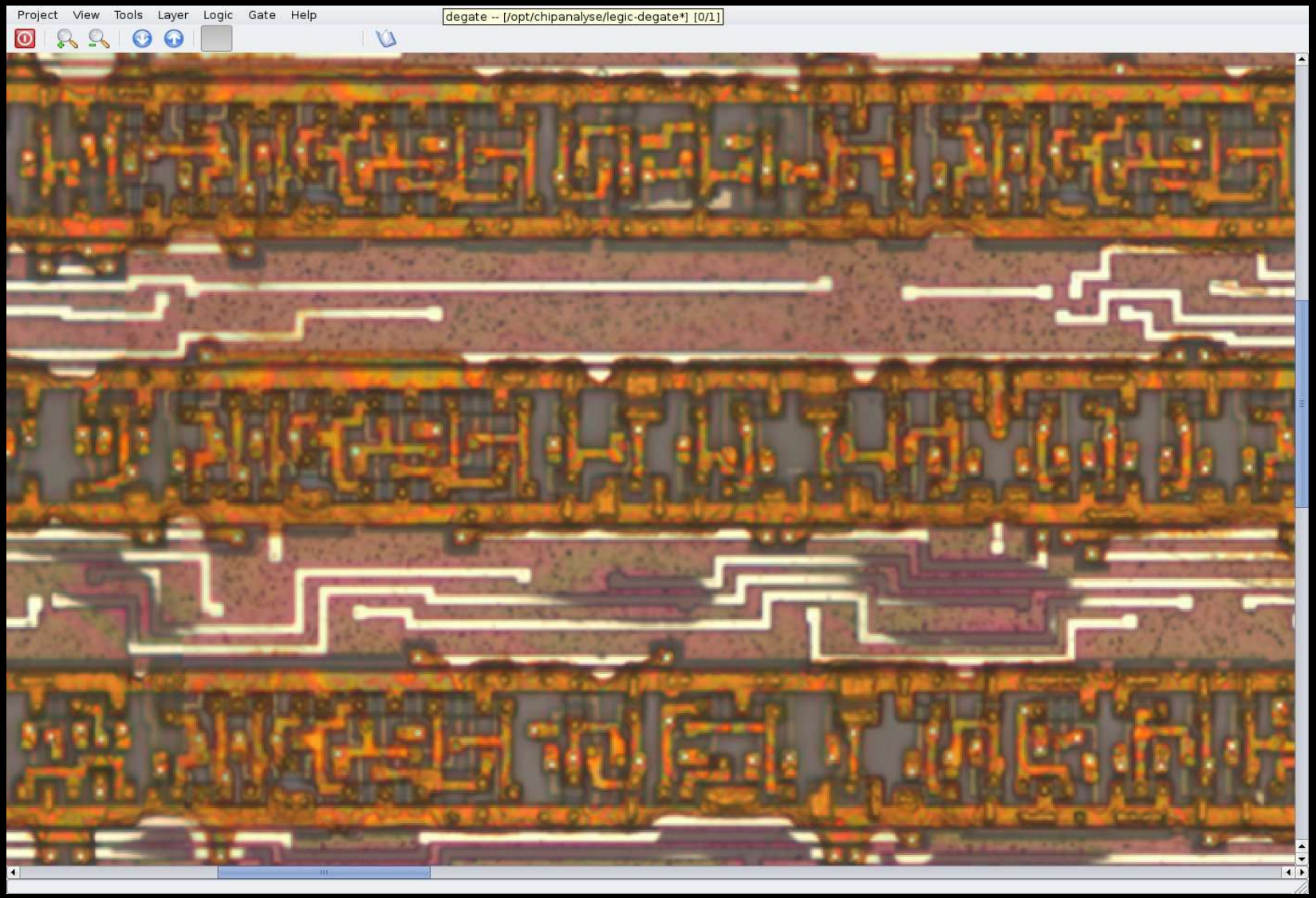
DECT

Automatisierte Gateerkennung

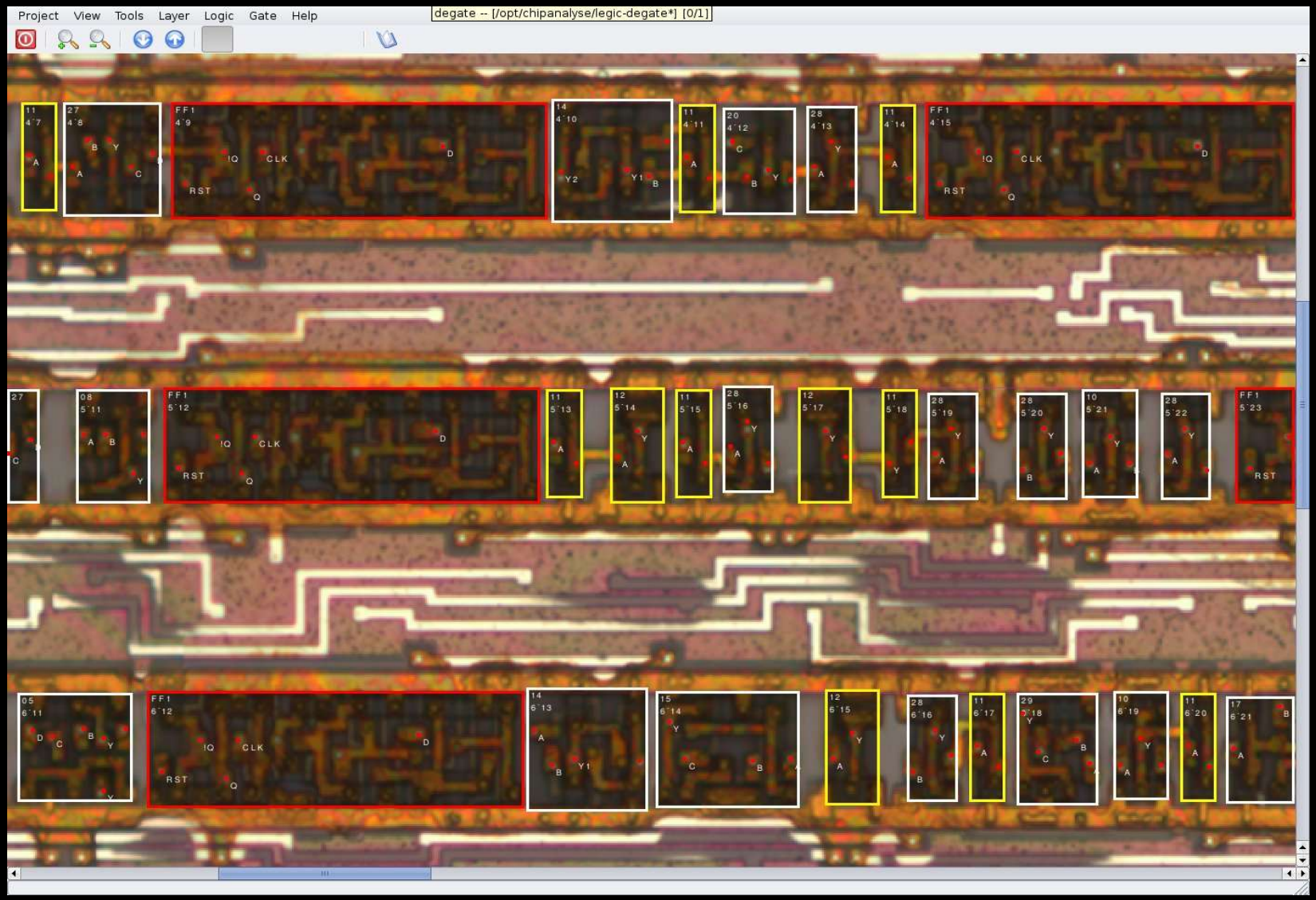


4 NAND:
Y = !(A & B & C & D)

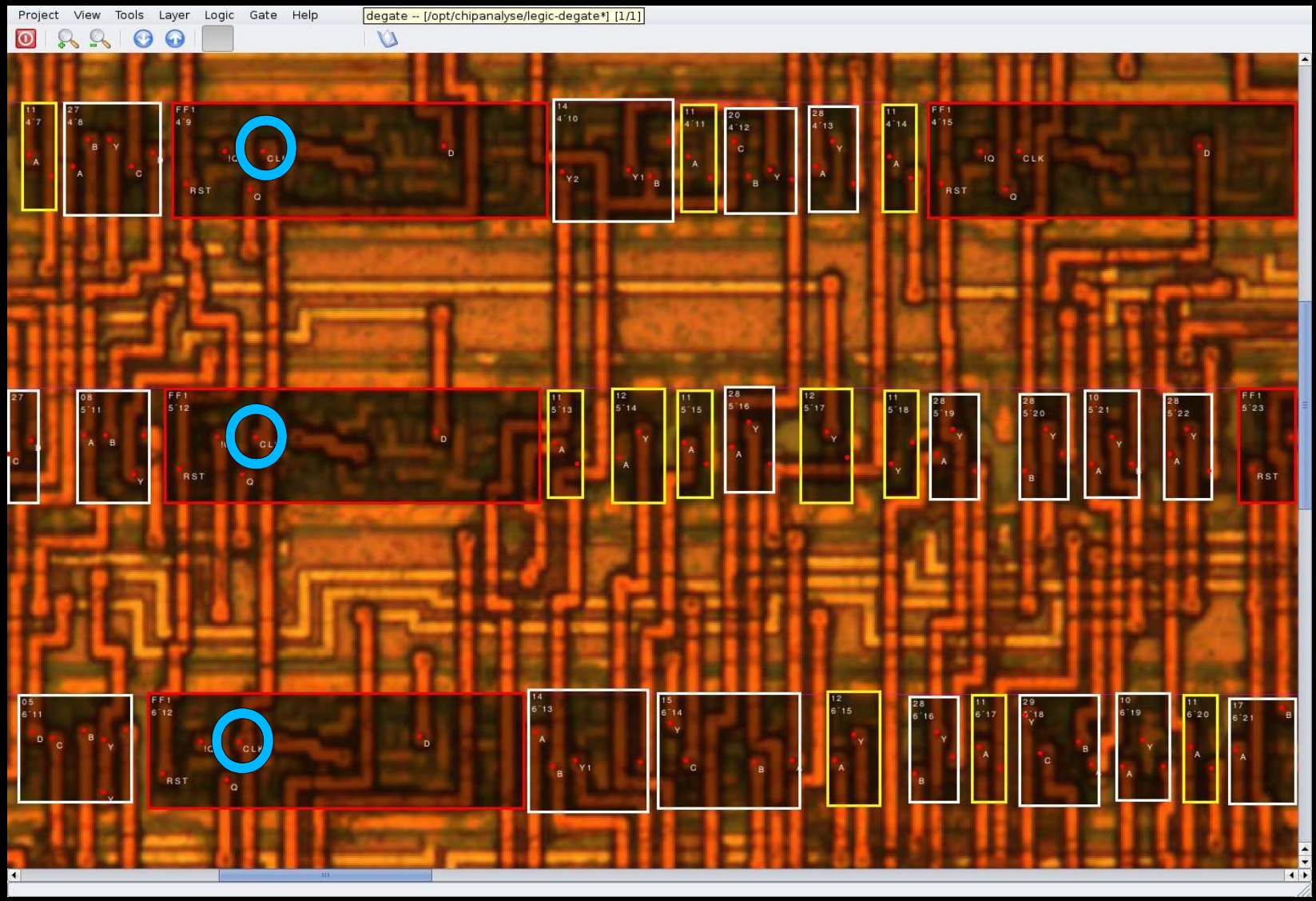
Automatisierte Gateerkennung



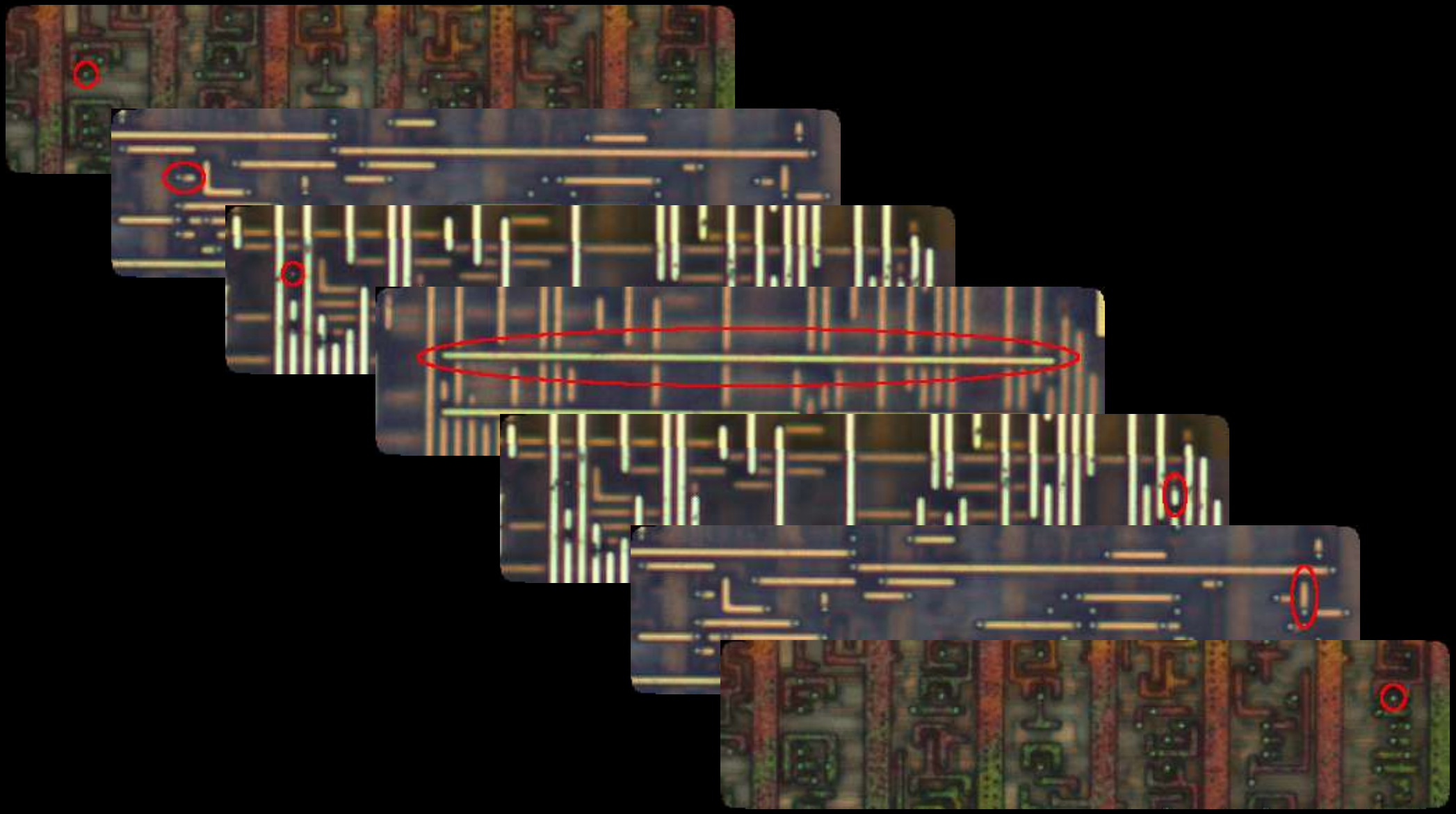
Automatisierte Gateerkennung



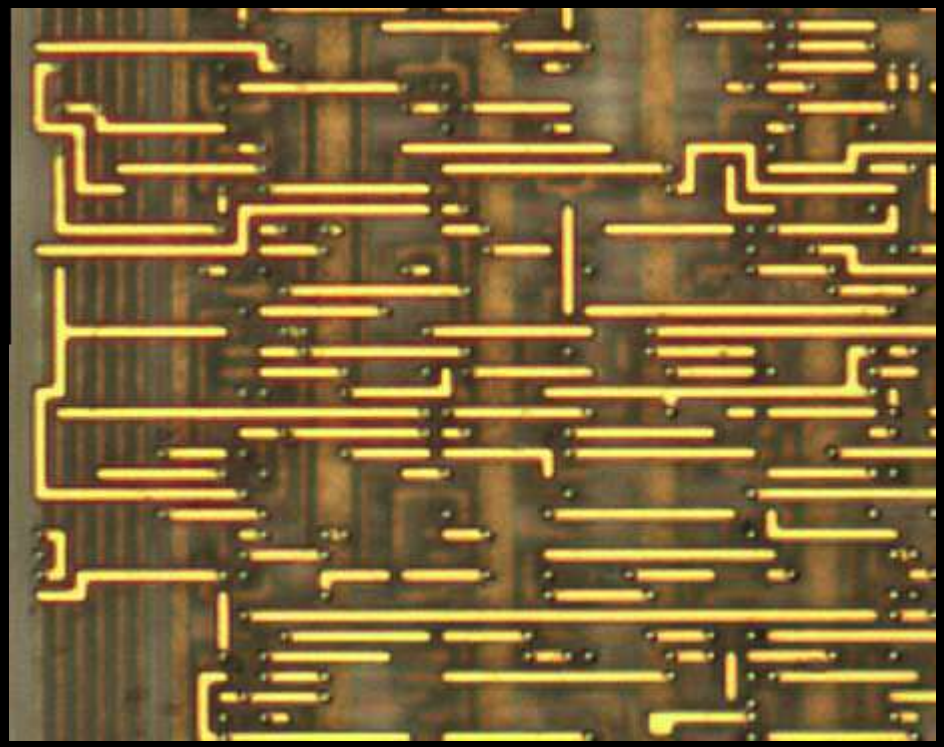
Manuelles Verfolgen der Interconnections

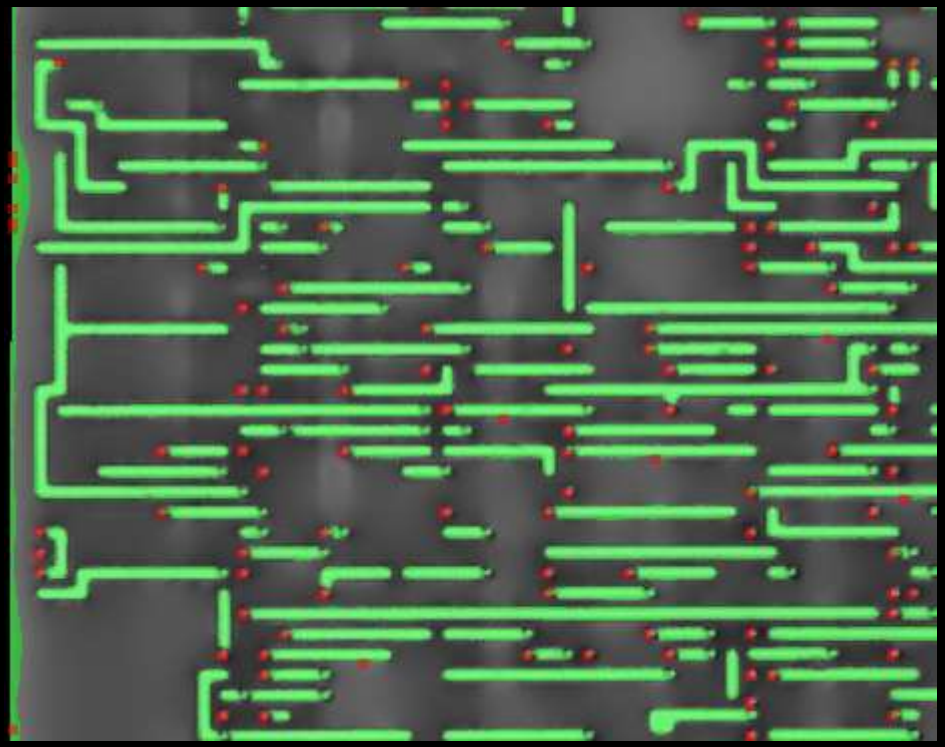


interconnections (MIFARE classic)

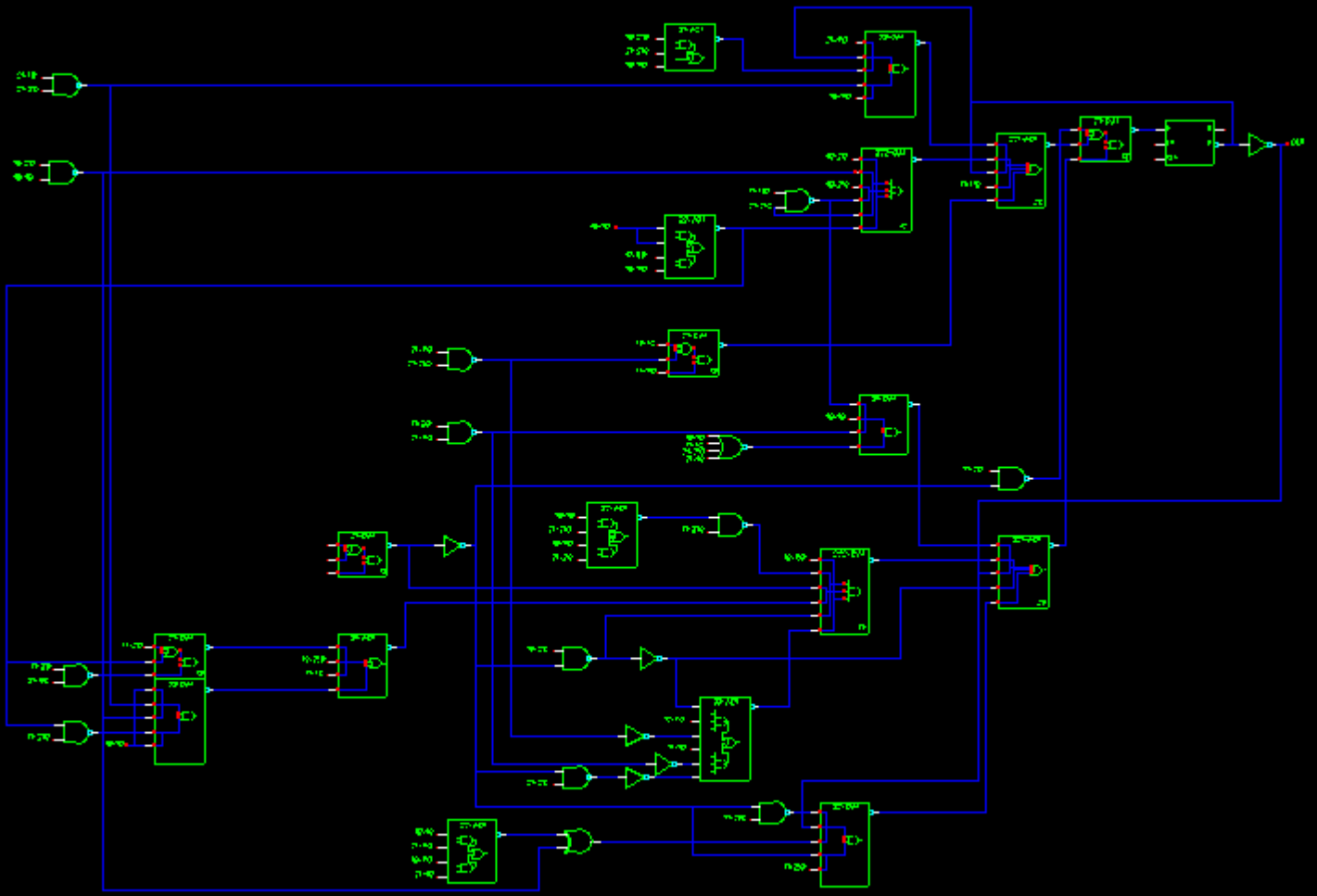


Automatisiertes Erkennen der Interconnections

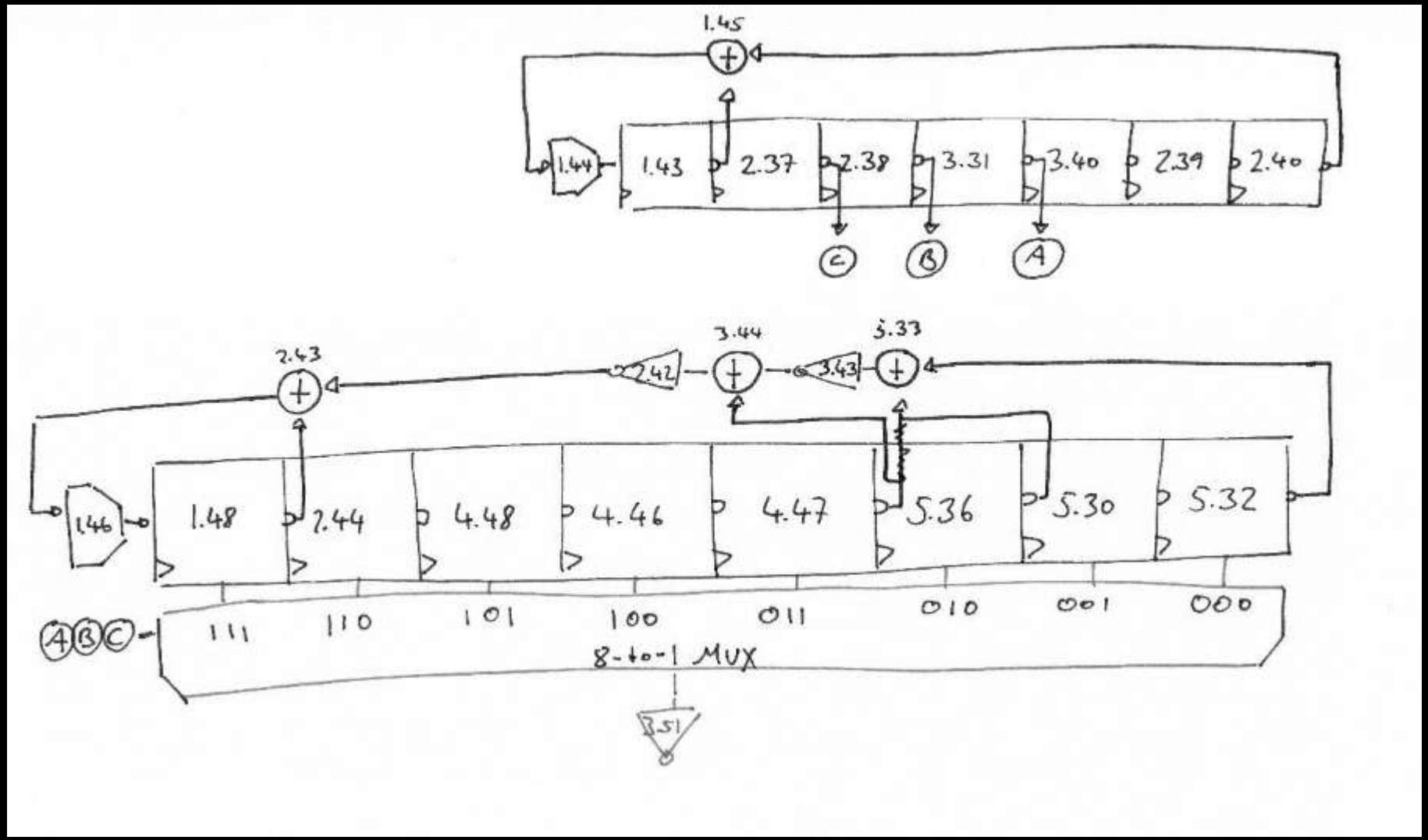




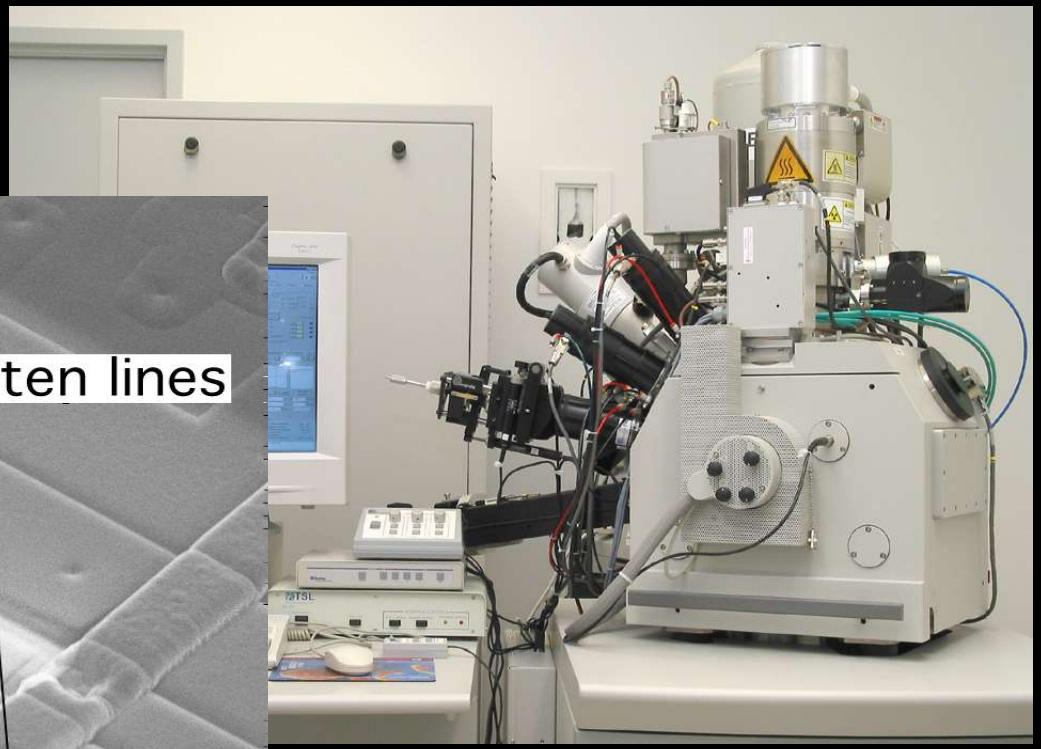
DSC - combinder

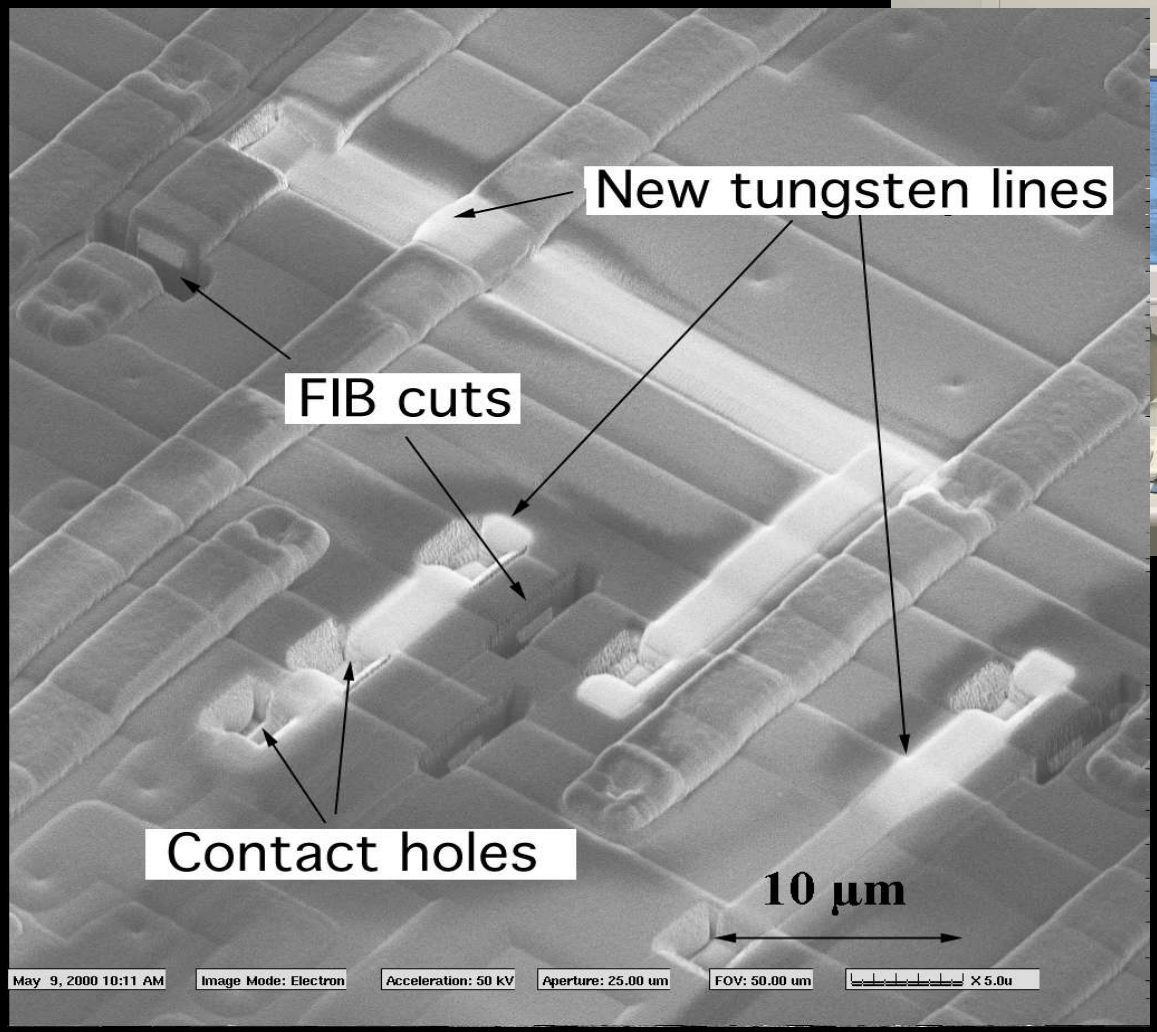


Legic Prime


1.45
1.44
1.43
2.37
2.38
3.31
3.40
2.39
2.40
C
B
A
2.43
2.42
3.44
3.43
5.33
1.46
1.48
2.44
4.48
4.46
4.47
5.36
5.30
5.32
A B C
111
110
101
100
011
010
001
000
8-to-1 MUX
3.51

Focused ion beam





Zusammenfassung

Reverse engineering von Microchips ist mit relativ geringem finanziellen und technischen Aufwand möglich.

Propritäre Cryptoalgorithmen bieten keinen Schutz.

Auch bei der Hardware security **offene Algorithen** verwenden!


vielen Dank!
starbug@ccc.de