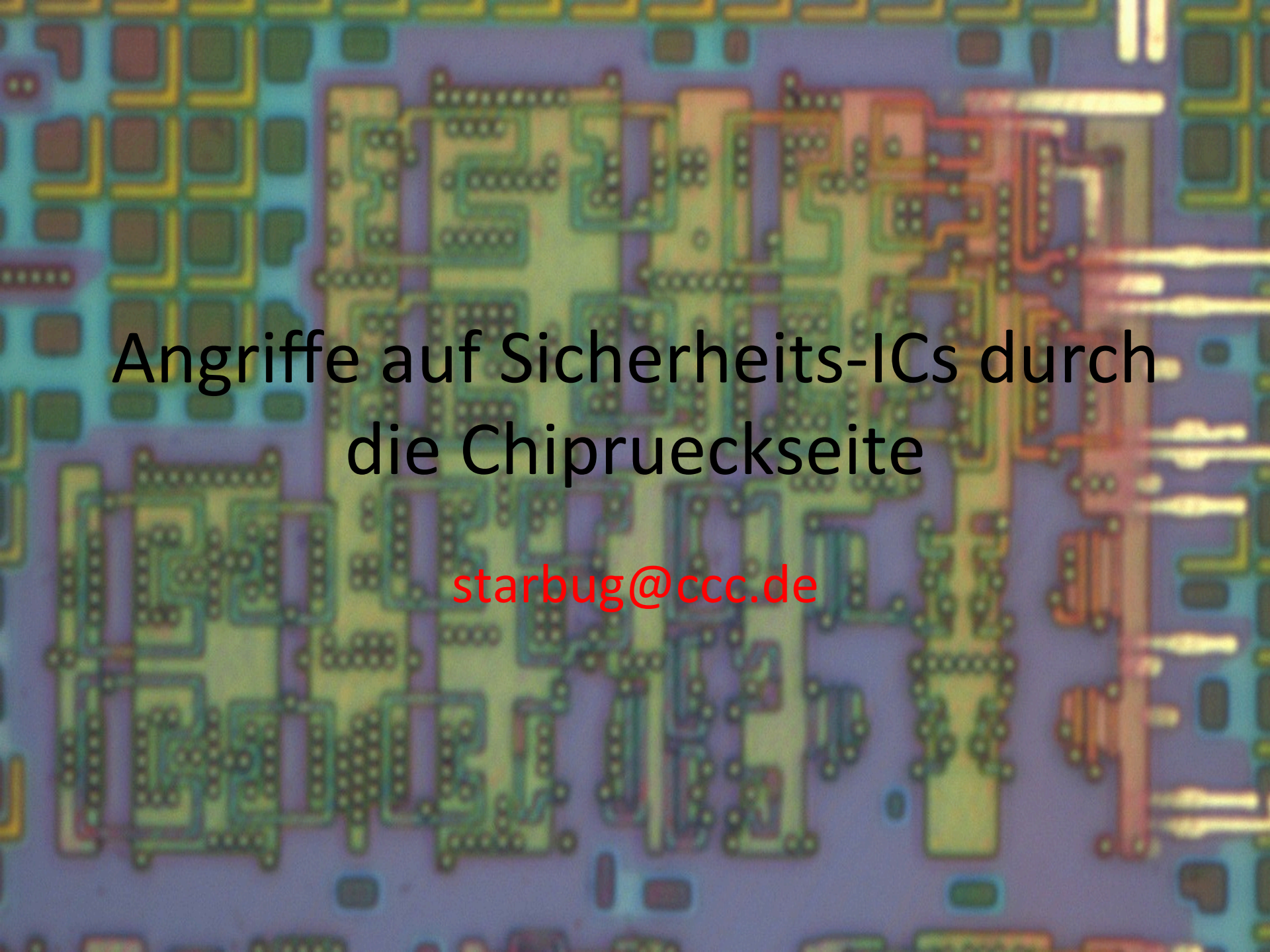
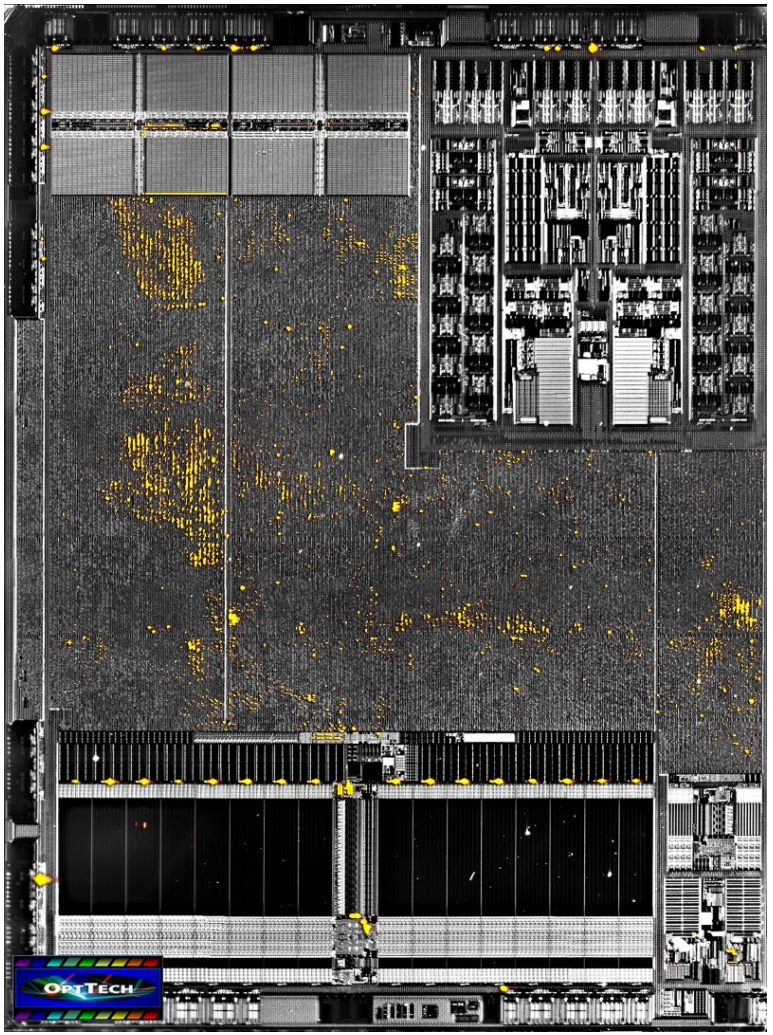


Angriffe auf Sicherheits-ICs durch die Chipruekseite

starbug@ccc.de

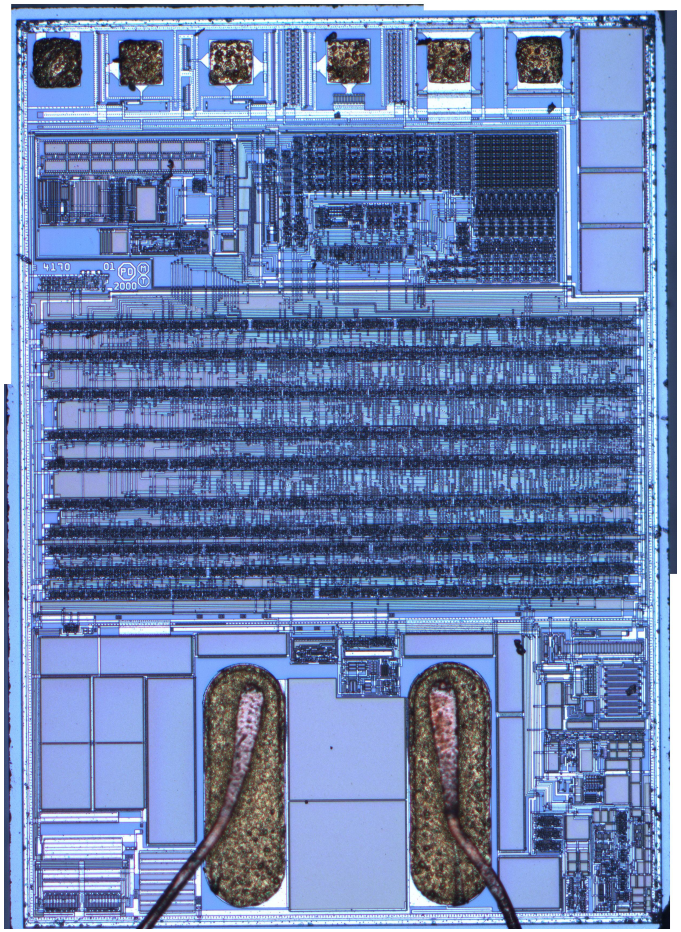
Inhalt

- Aufbau eines Chips
- Bisherige Angriffe
- Gegenmassnahmen
- Neue Angriffe

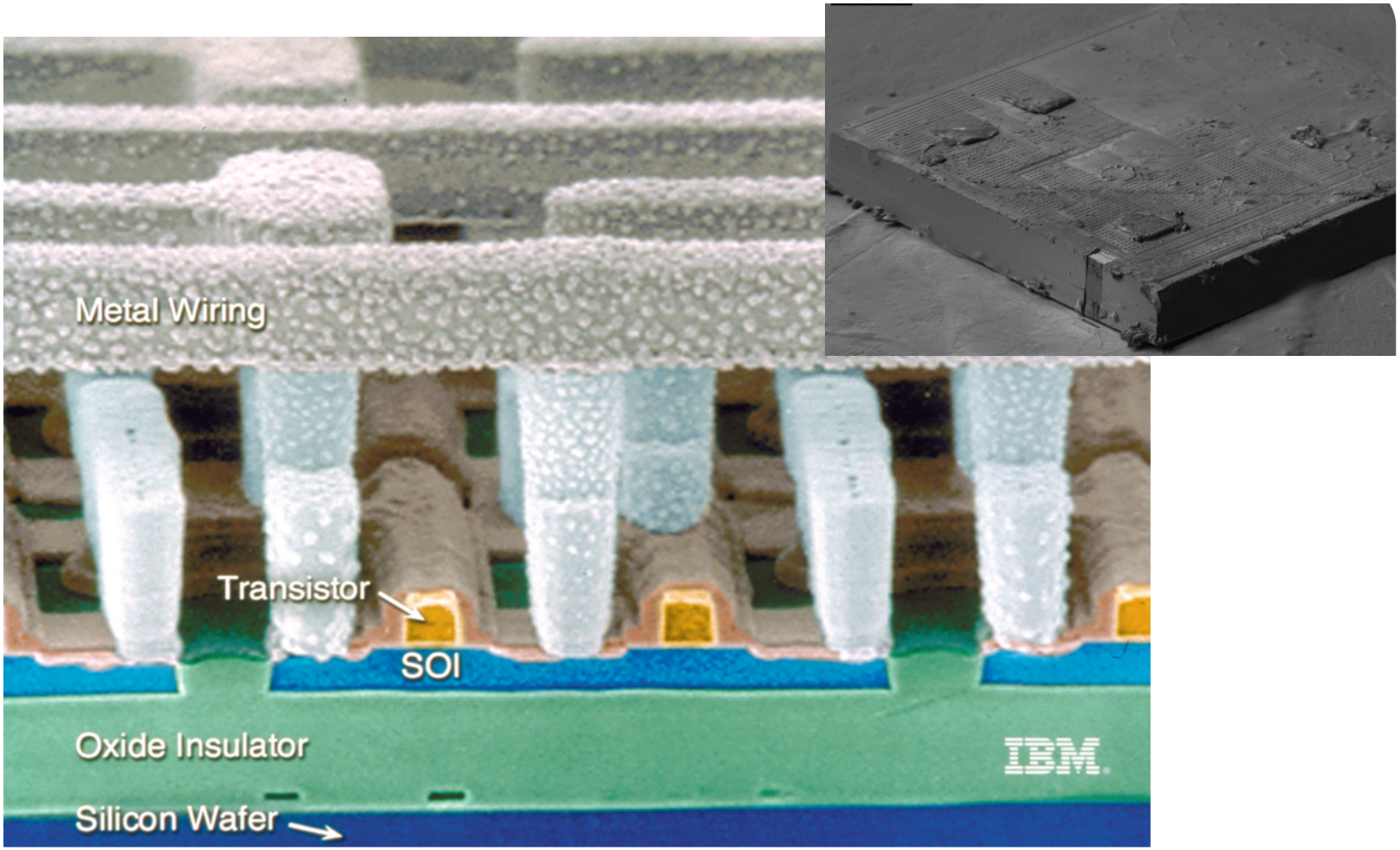


Horizontaler Aufbau

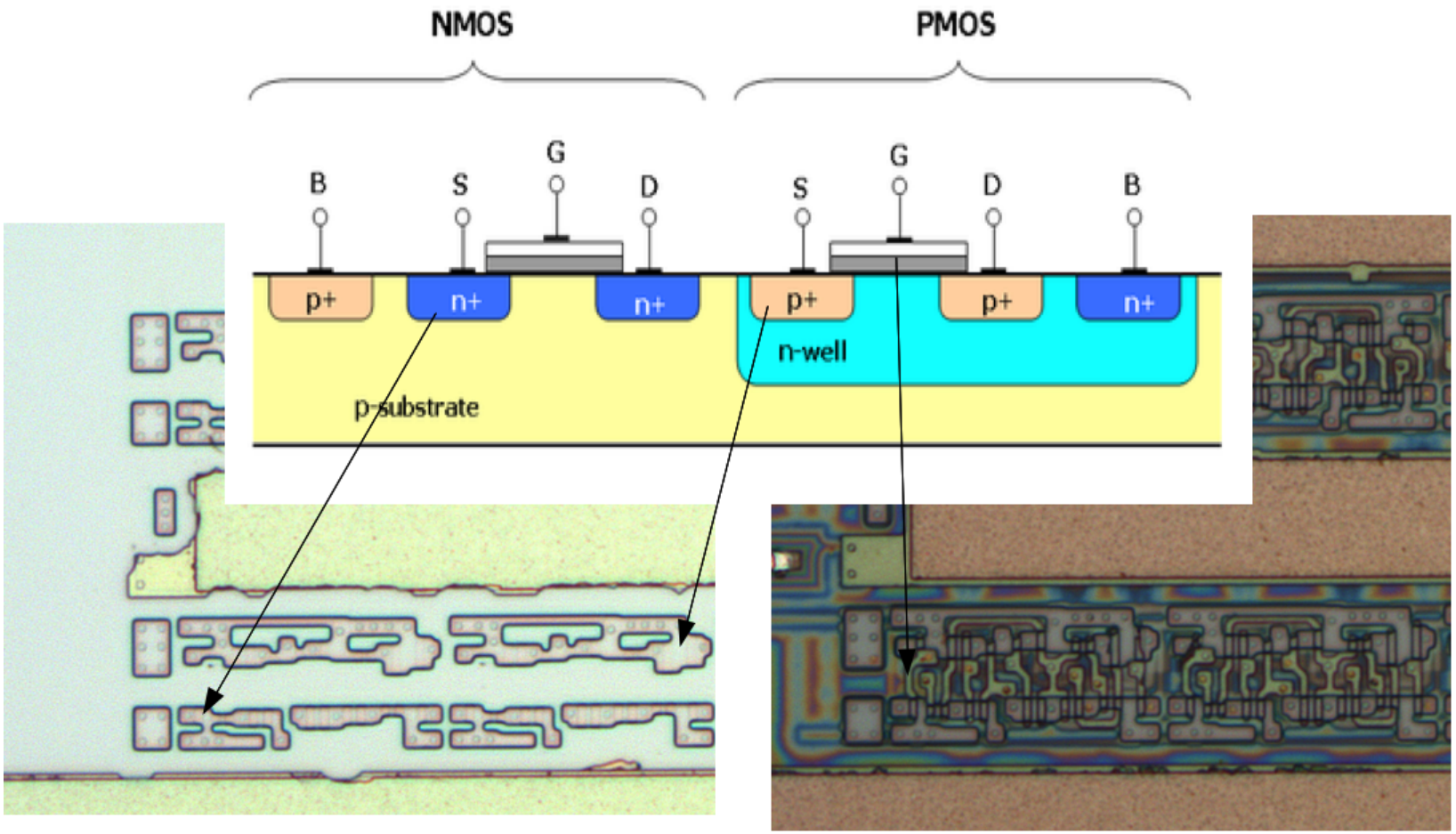
- Bond- / Testpads
- Memory
  - ROM/FLASH
- Analoge Parts
  - RF / Spannungsversorgung
- Digitale Teile
  - Protokoll
  - Krypto



Vertikaler Aufbau

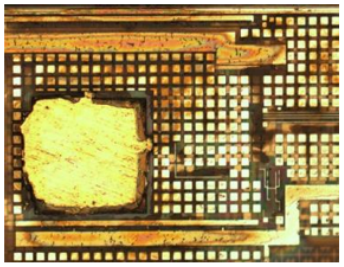


Transistoren



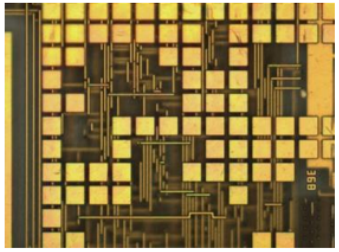
Layers

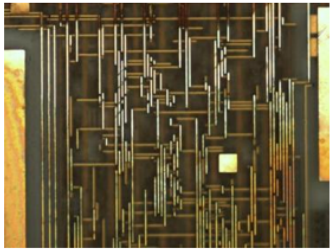
Layer

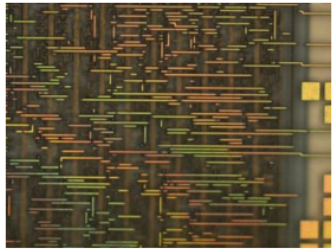


Cover Layer
(M5)

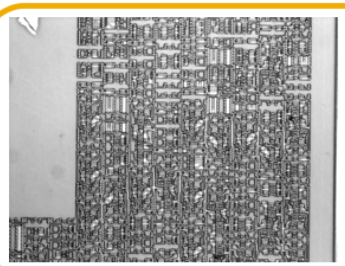
Interconnection Layer (M2-M4)







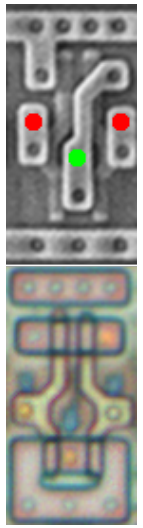
Logic
Layer
(M1)

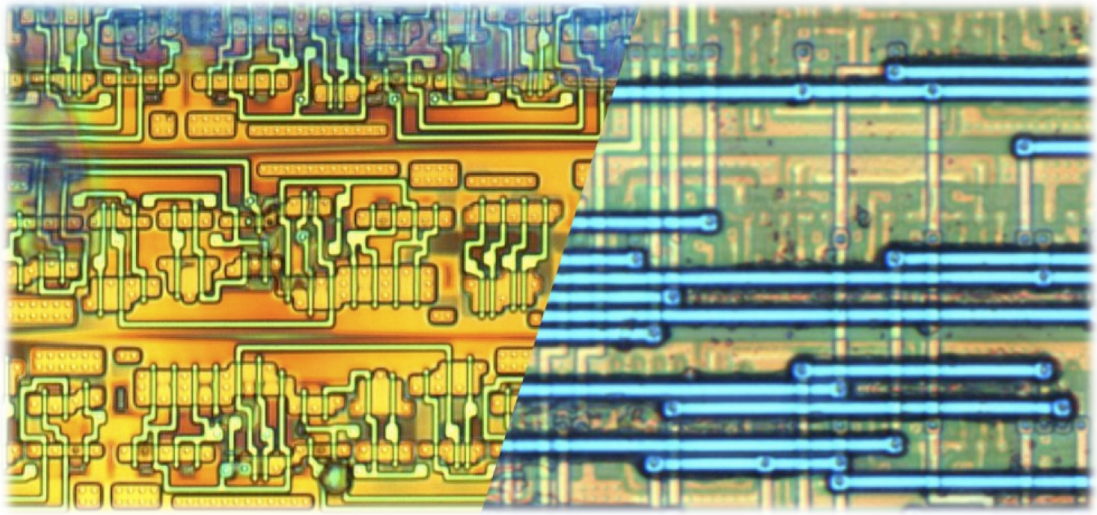


Transistor
Layer

Reversing propritaere HW

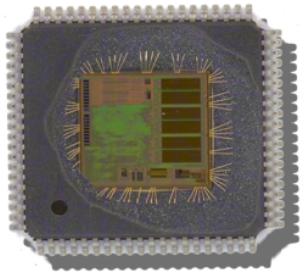
- Schichtweises Polieren
- Bilder machen
- Gates erkennen + Funktionen ermitteln
- Verbindungen tracen
- Krypto finden

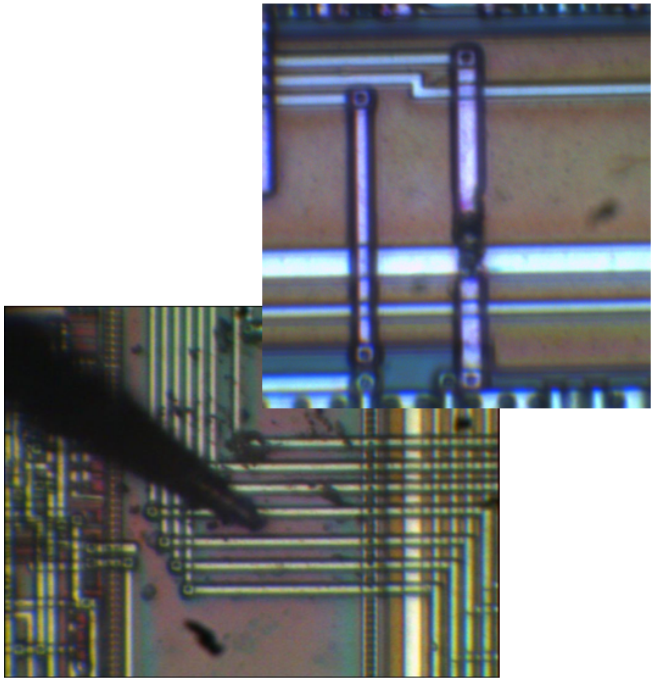




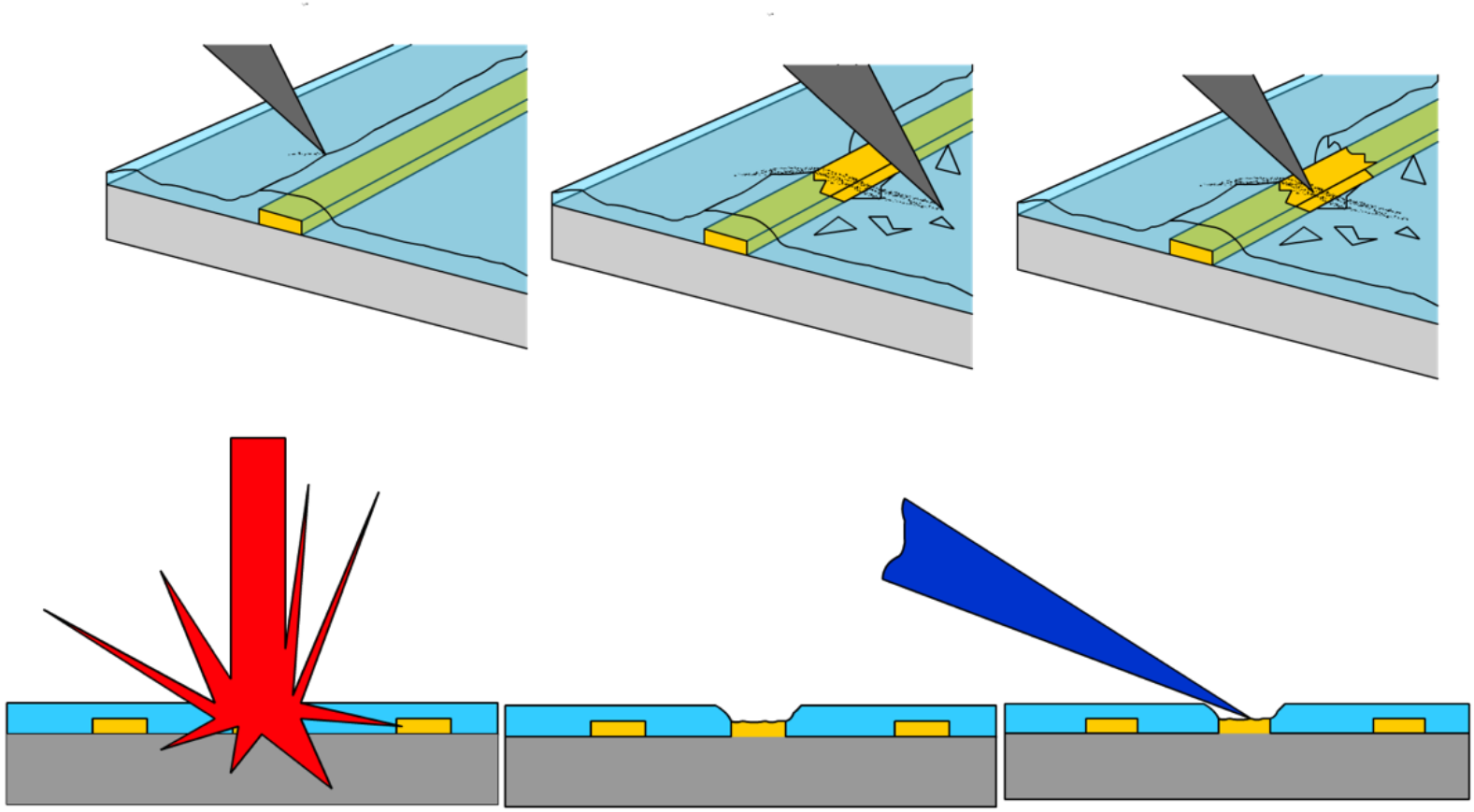
Probing

- Freilegen des Chips
  - Aetzen, Fraesen
- Entfernen der Passivierung
  - Laser, Scratching, FIB
- Probing
  - Auslesen des Speicherinhalts
  - Ueberpruefen von Ergebnissen des reverse engineering





Probing

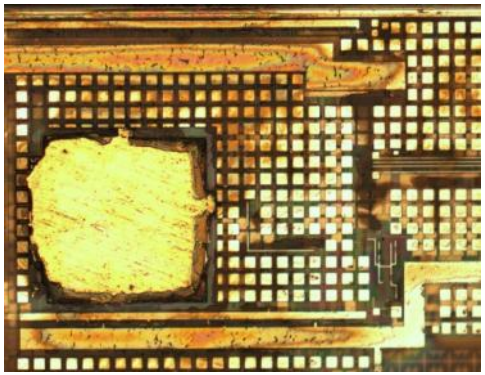


Gegenmassnahmen

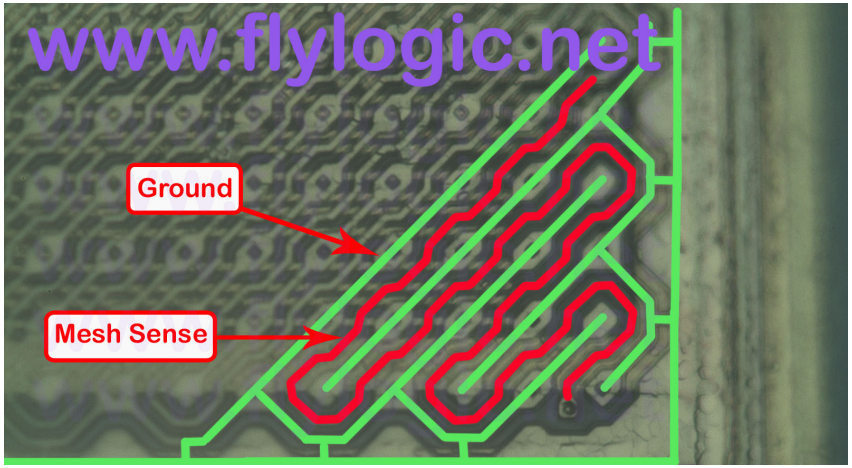
- Smartcards statt propritaere Krypto
- Shields
- Meshes
- verlegen der Datenleitungen
  - in tiefere Layer
  - unter Powerleitungen
- Sensoren

Meshes / Shields

- Shield: passiv
  - Sichtschutz
  - Verhindert Fuse Reset



- Mesh: aktiv
  - Verhindert Probing



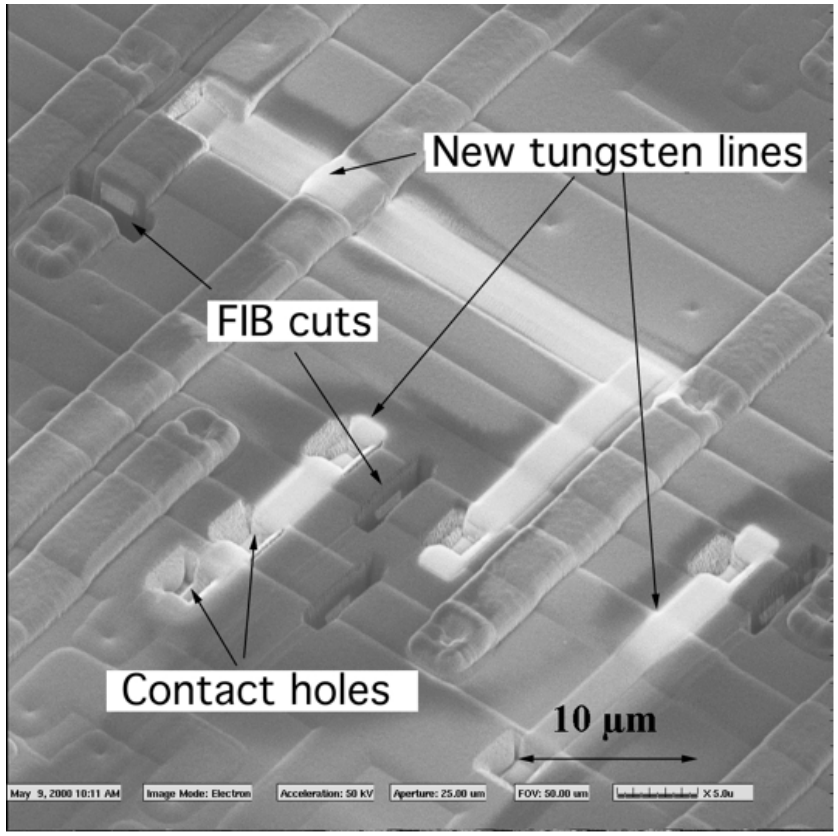
Sensoren

- Licht
  - UV, Laser
- Strom (brownout)
- Temperatur
- Taktrate
- Elektrische Aufladung (FIB)

Focused Ion Beam FTW

- Abtragen von Chipmaterial
- Abscheiden von leitendem und isolierendem Material
- Spotsize ~10nm

- Durchtrennen von Leitern
- Schaffen neuer Verbindungen
- Kontaktieren tieferer Layer

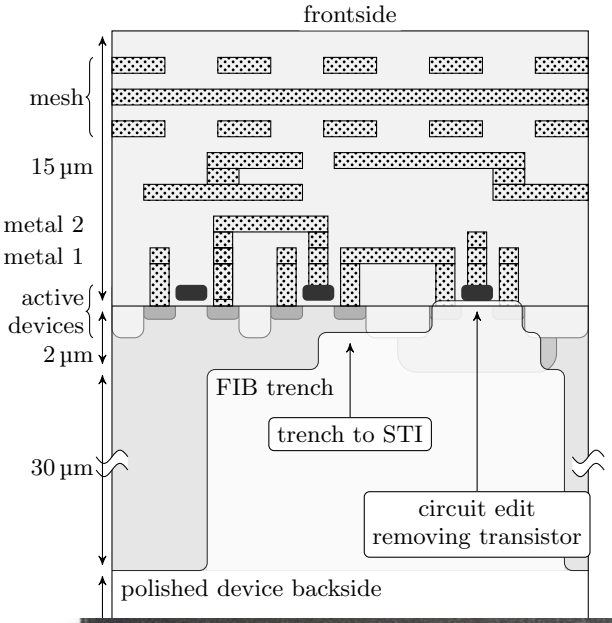


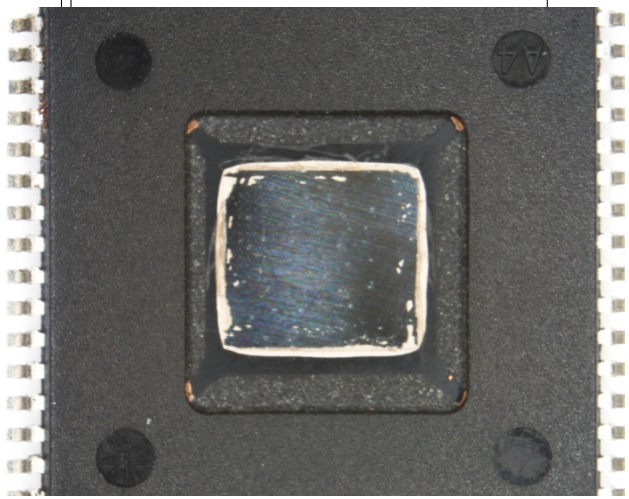
Gegenmassnahmen

- Shields
- Meshes
- verlegen der Datenleitungen
  - in tiefere Layer
  - unter Powerleitungen
- Sensoren
- => die Rueckseite

Praeparierung

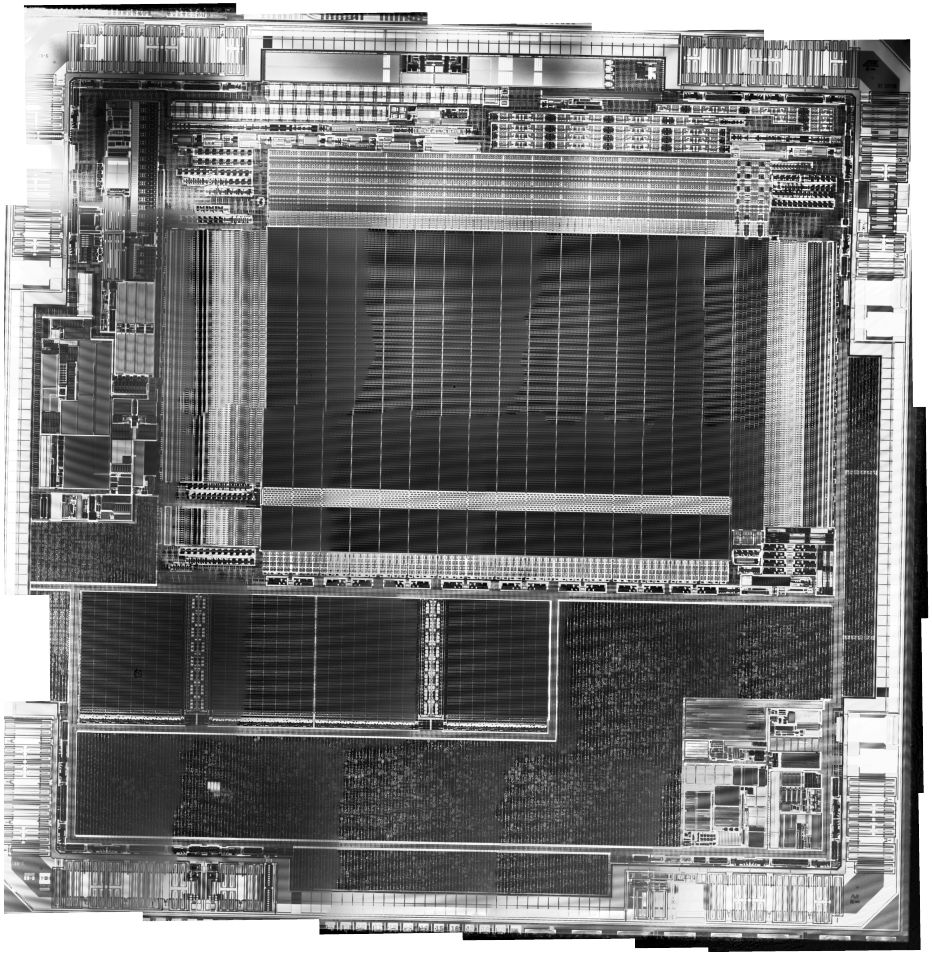
- Fraesen des Gehaeuses und des Siliziumsubstrats
- Grossflaechiges FIB-Aetzen
- Gezieltes FIB-Aetzen





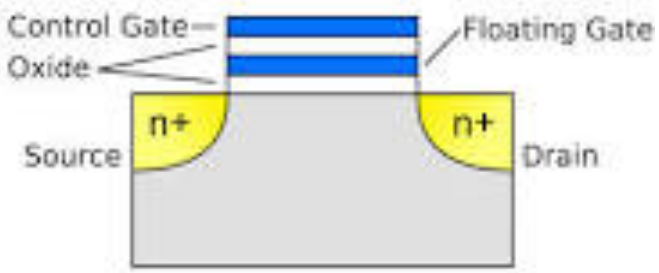
Bilder durch die Rueckseite

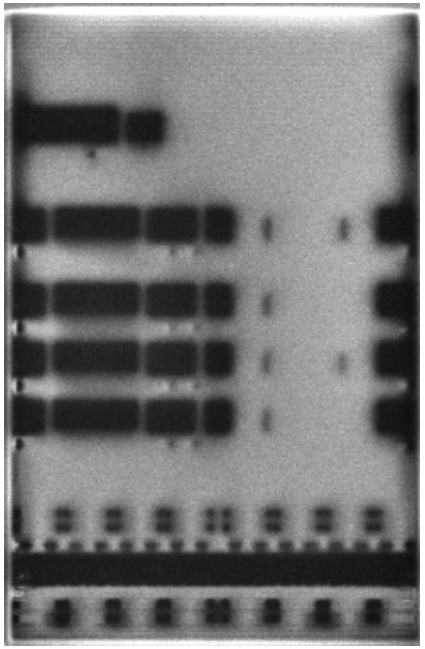
- Silizium fuer Wellenlaengen > 1100nm transparent
- Illuminieren mit IR
- Detektion mit IR-Kamera
- Kein Schleifen
- Geringe Aufloesung

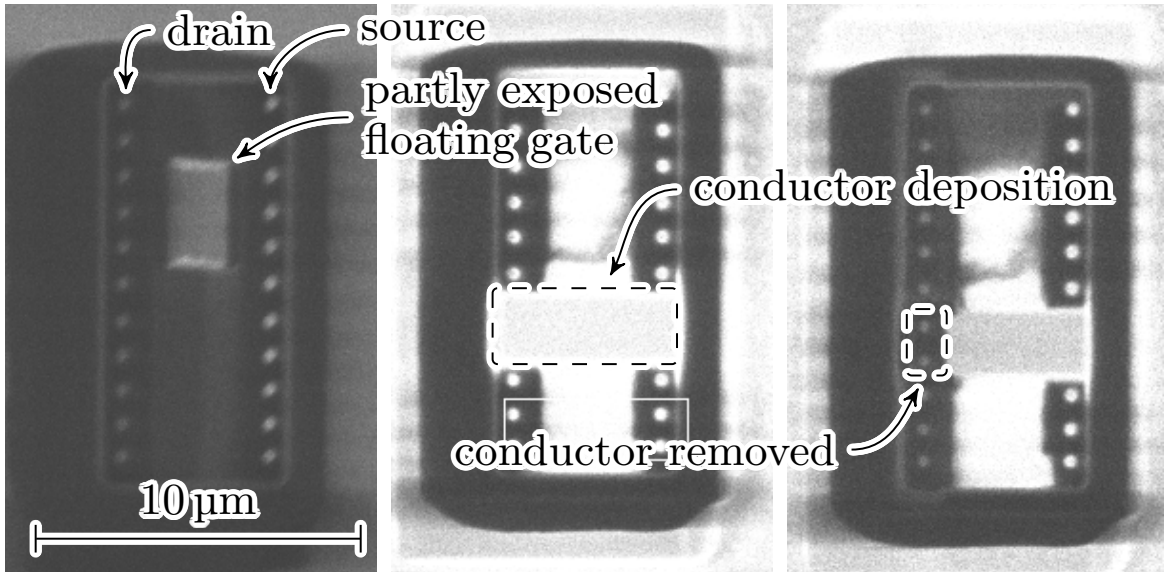


Fuses

- Floating Gate Transistoren
- Trennen oder Verbinden von source und drain
- Aufladen des Gates

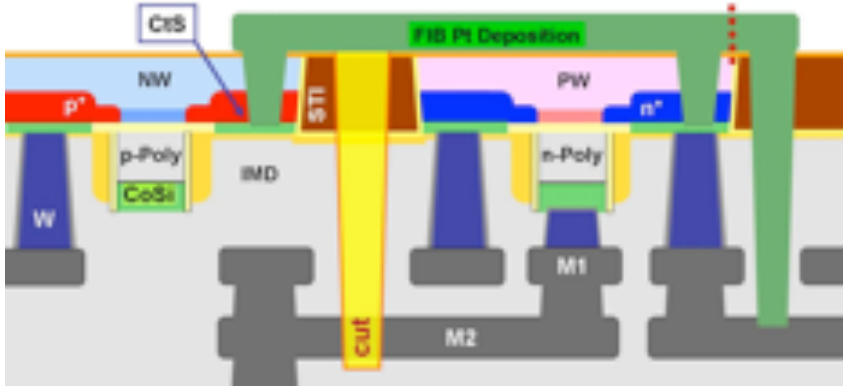






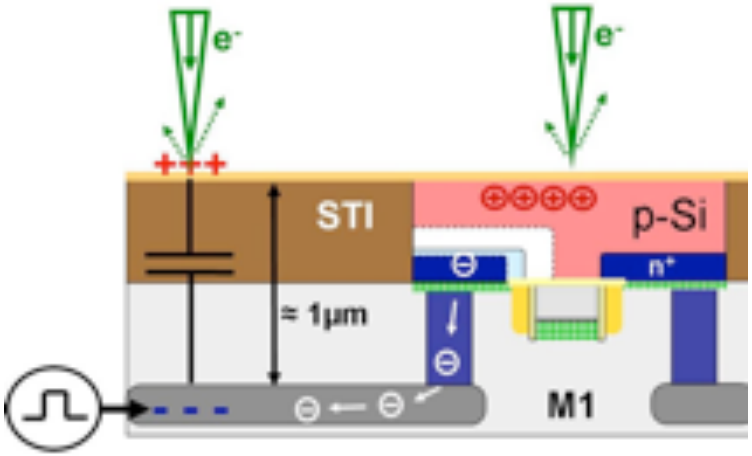
Backside probing

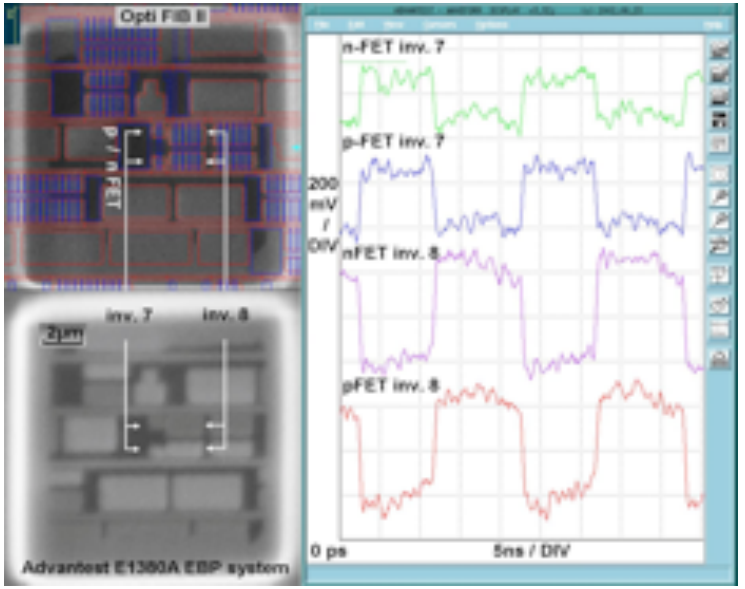
- Keine Meshes / Shields
- Datenleitungen in M1 / M2
- Selbst Transistoren direkt kontaktierbar



E-beam probing

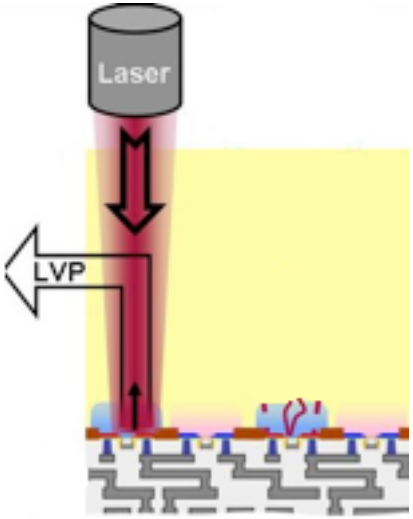
- Signale aus Metal1 “sichtbar” an der Rueckseite
  - Capacitive coupled voltage contrast
- Spotsize Transistorgroesse





Laser Voltage Probing

- Bestrahlen mit IR Laser
- Signale des Chips werden auf reflektiertes Licht aufmoduliert
- Auslesen von Speicher
  - Laserinduzierte Schwankung der Versorgungsspannung



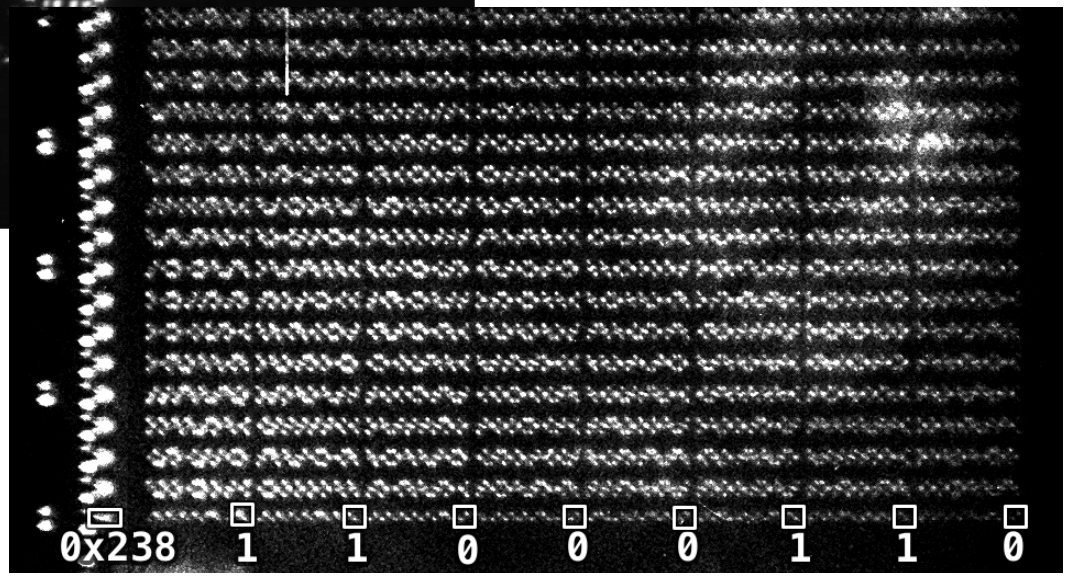
Optical Side channel

- Schaltende Transistoren senden Licht aus (hot carrier luminiszenz, grosses elektrisches Feld)
- Geringe Anzahl von Photonen
  - erhoehung der kinetischen Energie (Spannung)
  - Duenneres Substrat
  - Integration des Signals
  - IR Detektoren
- CCD (grosse Flaeche, geringe Framerate)
- Single photon detectors (Einzeltransistorendetektion, 10ps Aufloesung)

Video

- Hier haette jetzt ein Video kommen koennen, wenn ich nicht zu bloed gewesen waere ein Video in Powerpoint zu integrieren. :P

Optical Side Channel



Optical fault injection

- Toggeln von Einzeltransistoren (Logic oder Speicher)
  - Bit-Flips in SRAM-Zellen (AES)
  - Clock glitching
- How the fuck does it work?
  - Fokusierter Laserstrahl
  - 1064 nm
  - Hohe Energie ca. 1 W