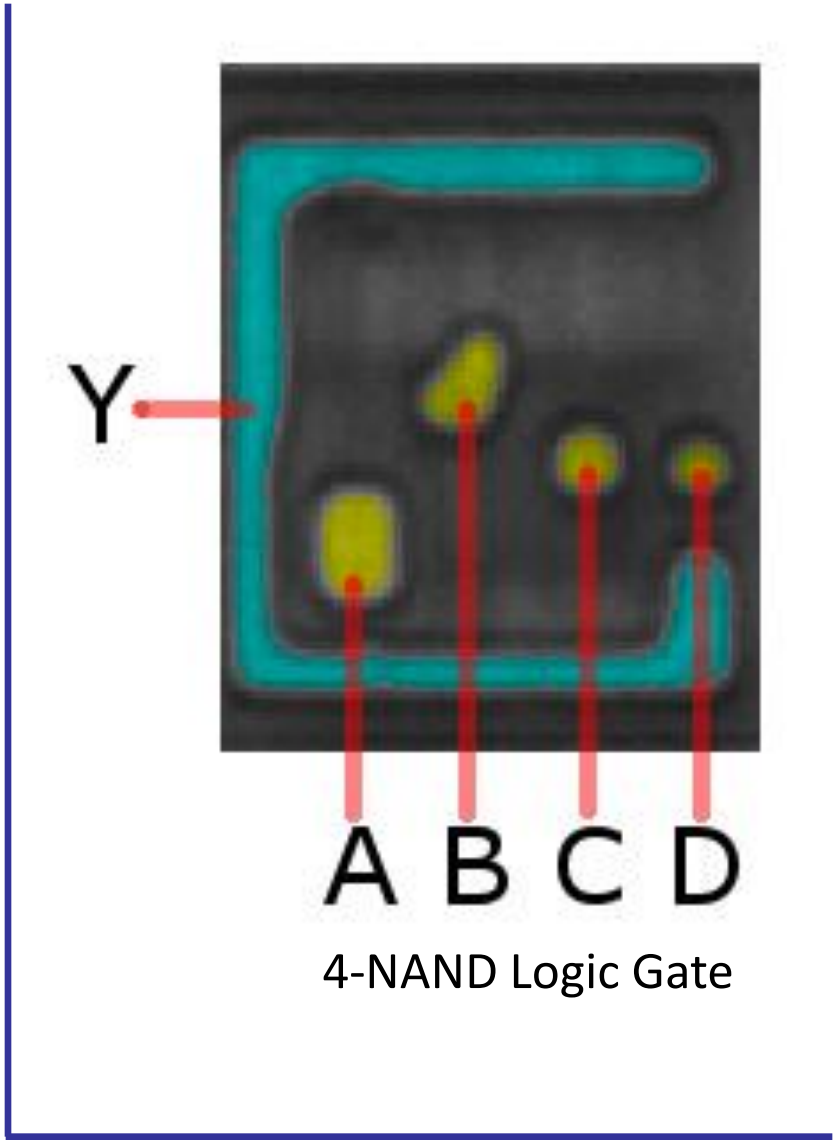
Deep Silicon Analysis

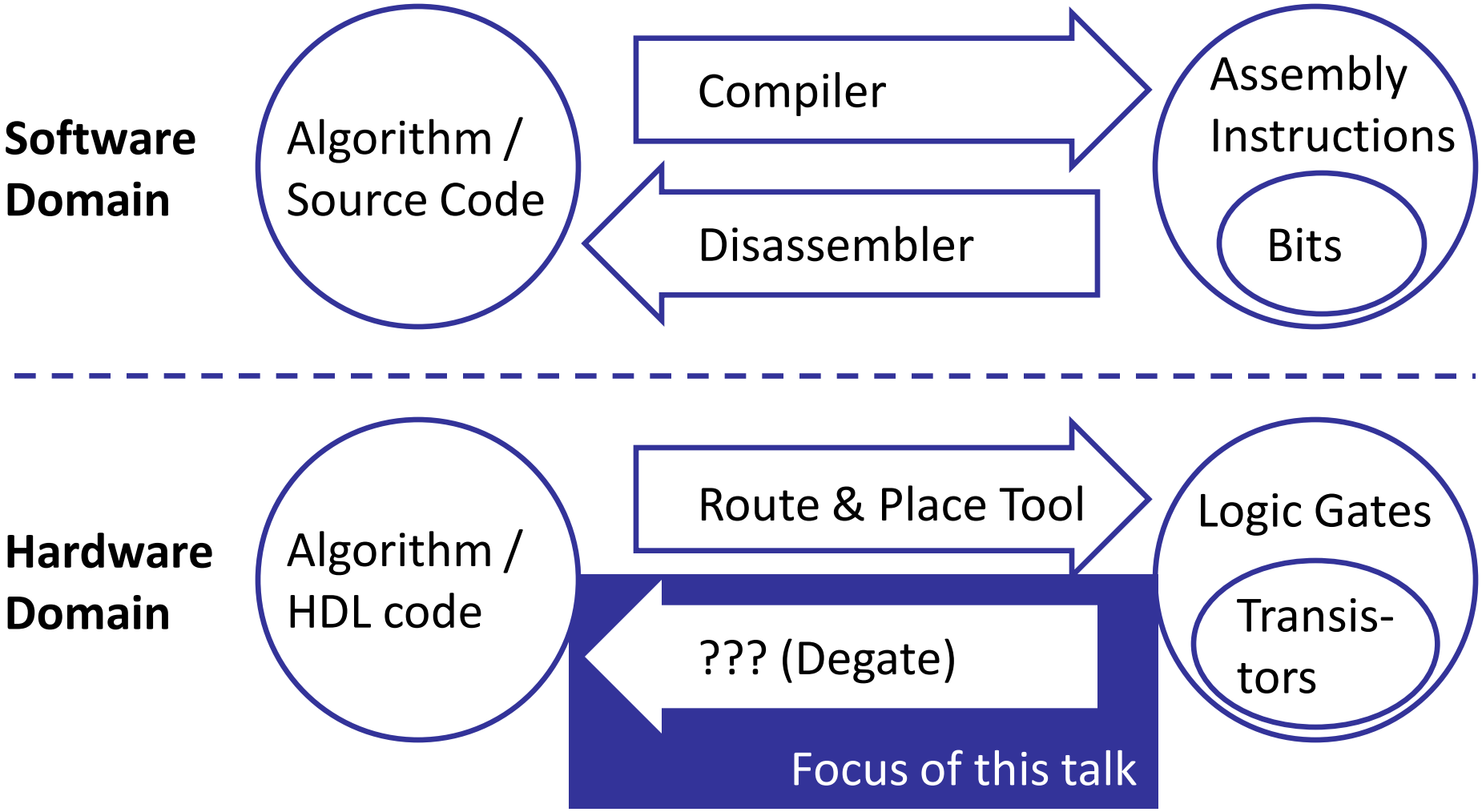
Karsten Nohl
& Starbug

@ HAR 2009



4-NAND Logic Gate

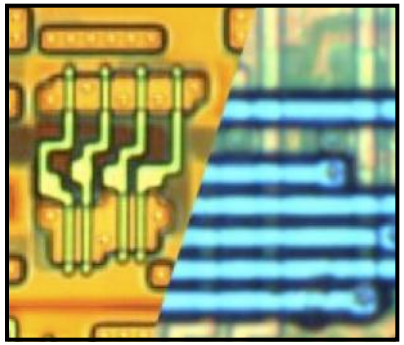
Hardware needs to become easier to analyze for hackers



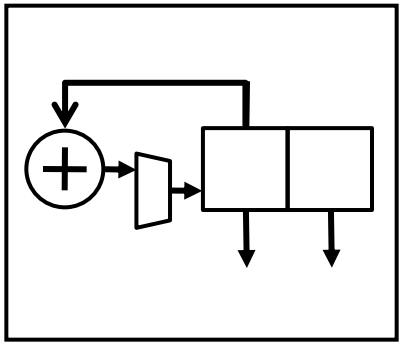
Algorithms can be extracted from chips in a 3-step process

Silicon disassembling process

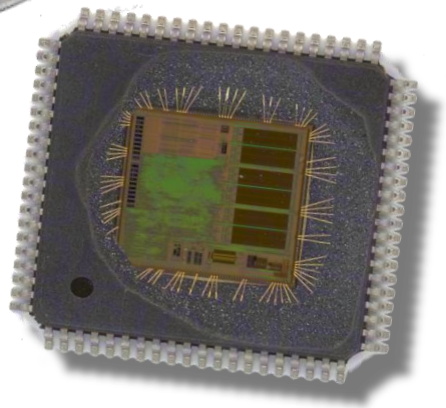
Imaging chips	Recognizing structures	Interpreting structures	Algorithm
▪ Polishing ▪ Microscoping ▪ Stitching	▪ Pattern recog. ▪ Wire tracing	▪ Gate simula-tion	
Silicon Chip	Chip images	Netlist	Annotated netlist



```
<?xml version="1.0"
<gate-library>
 <gate description=
  <ports>
   <port id="0" nam
   <port id="1" nam
```

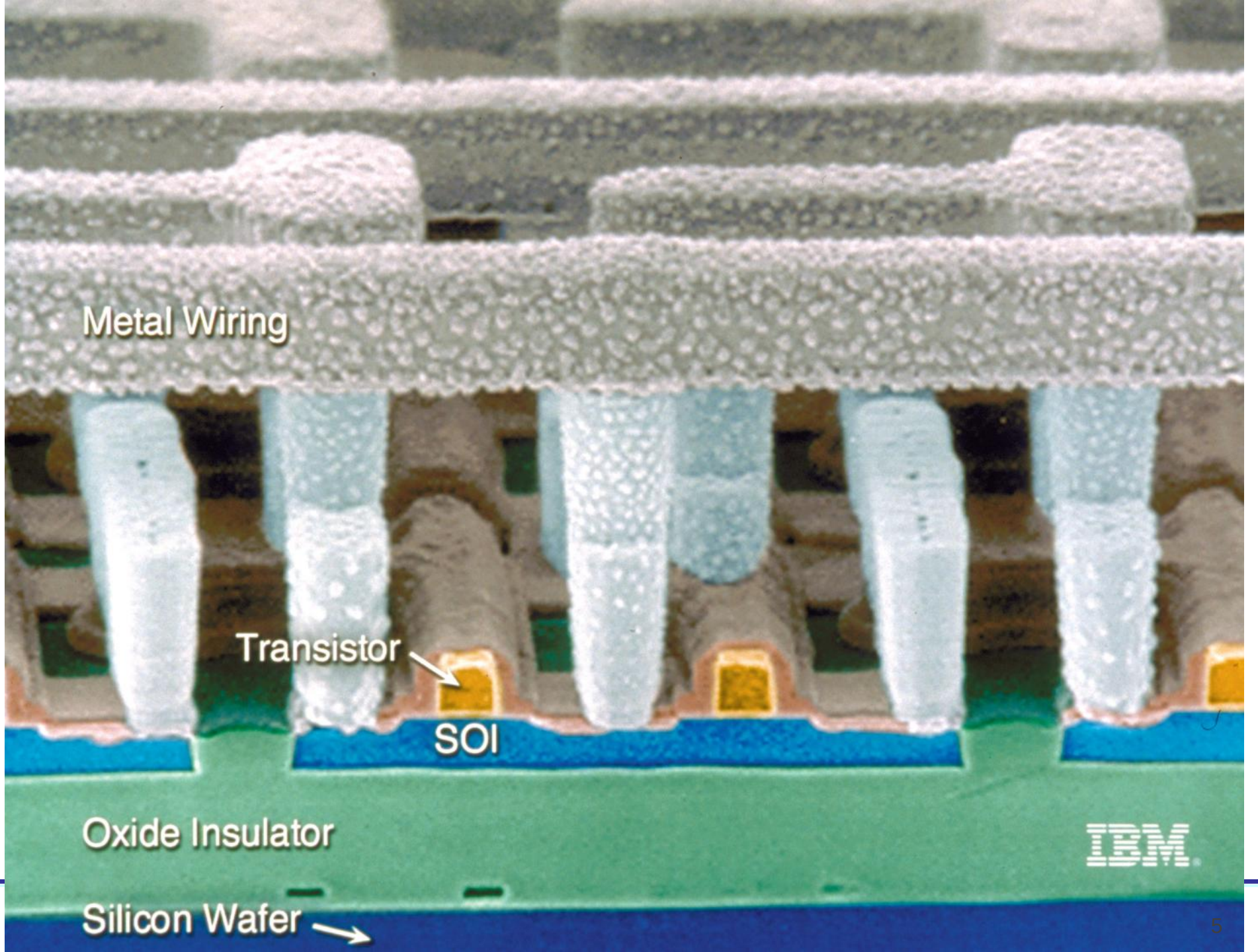


As preparation, chips are etched out from plastic containers



Chemically extract chips:

- Acetone
- Fuming nitric acid


Metal Wiring
Transistor
SOI
Oxide Insulator
IBM
Silicon Wafer

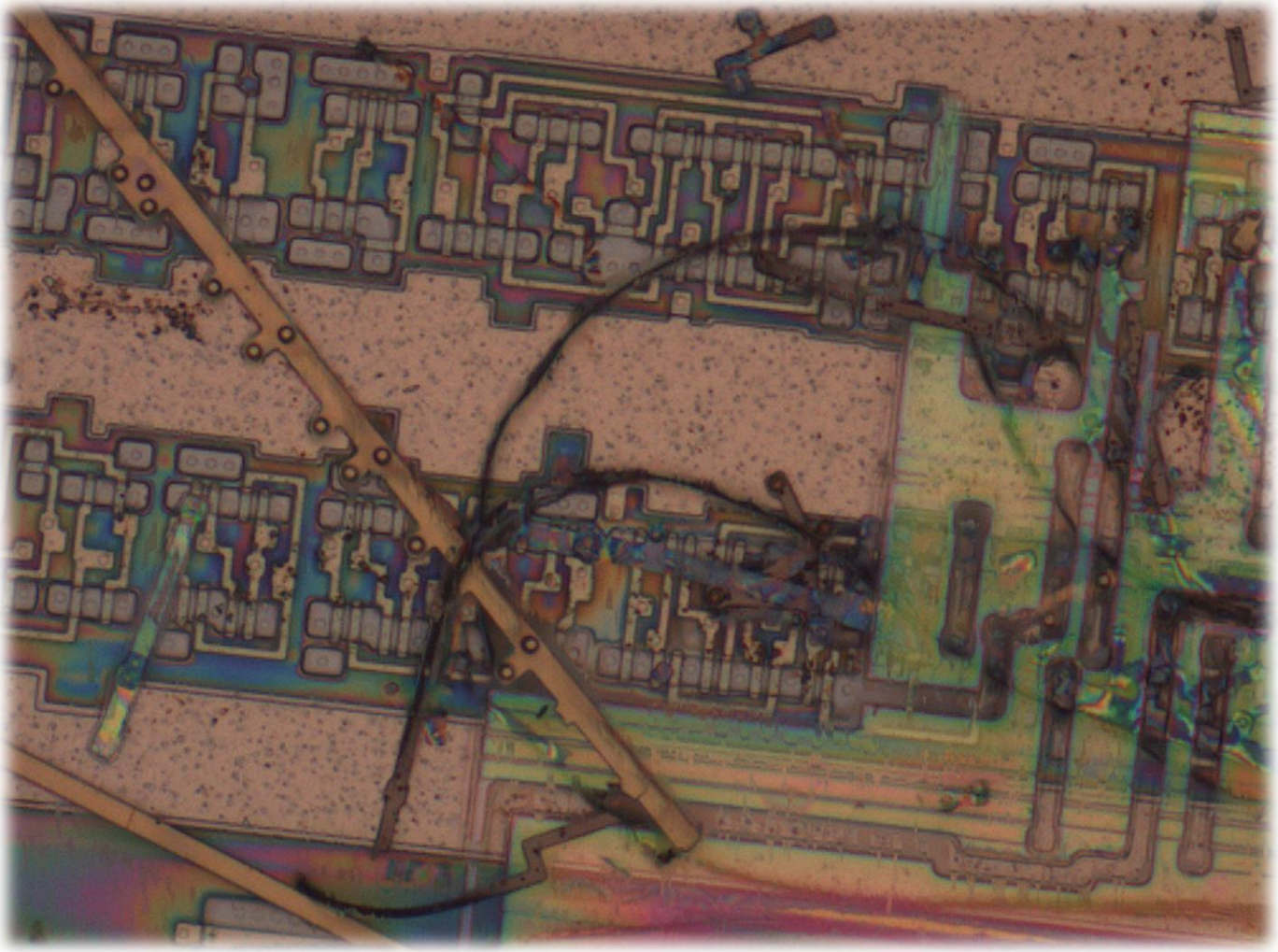
Chip dies are polished to reveal circuits

Polishing:

- Automated with machine
- Manually with sand paper

- Potential problem: tilt
- Solution: glue chip to block of plastic

Alternatively, HF etching removes the glass between metal layers

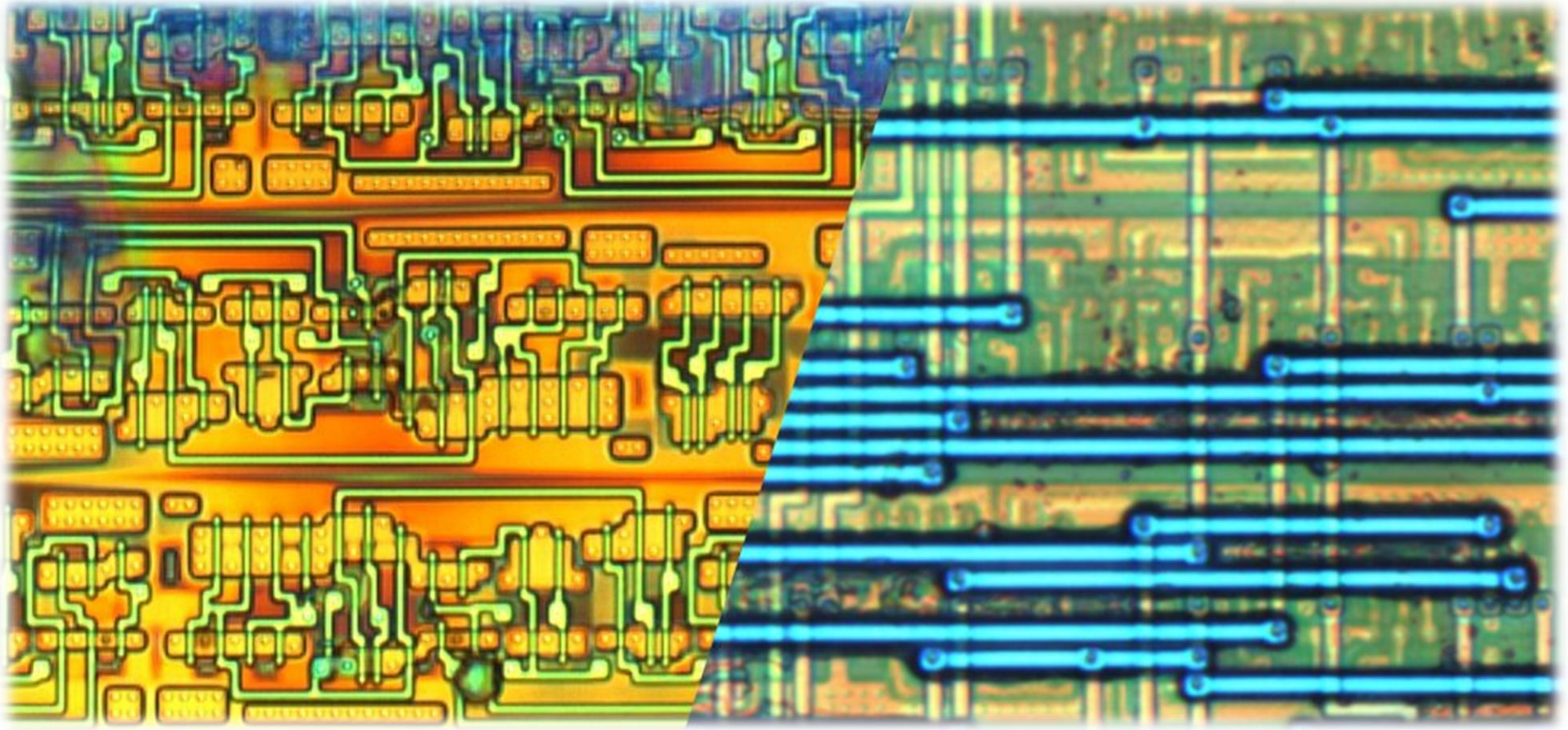


Each layer is imaged using an optical microscope

- Simple optical microscope
  - 500x magnification
  - Camera with 1 Mpixel
  - Costs < $1000

    — or—
- Confocal microscope
  - Colors images by depth
  - Makes structures easy to spot
  - Expensive: > $10k

Confocal microscopy preserves useful 3D information



Newer chips may require imaging resolutions below optical

Imaged using focused ion beam (FIB) with nm resolution

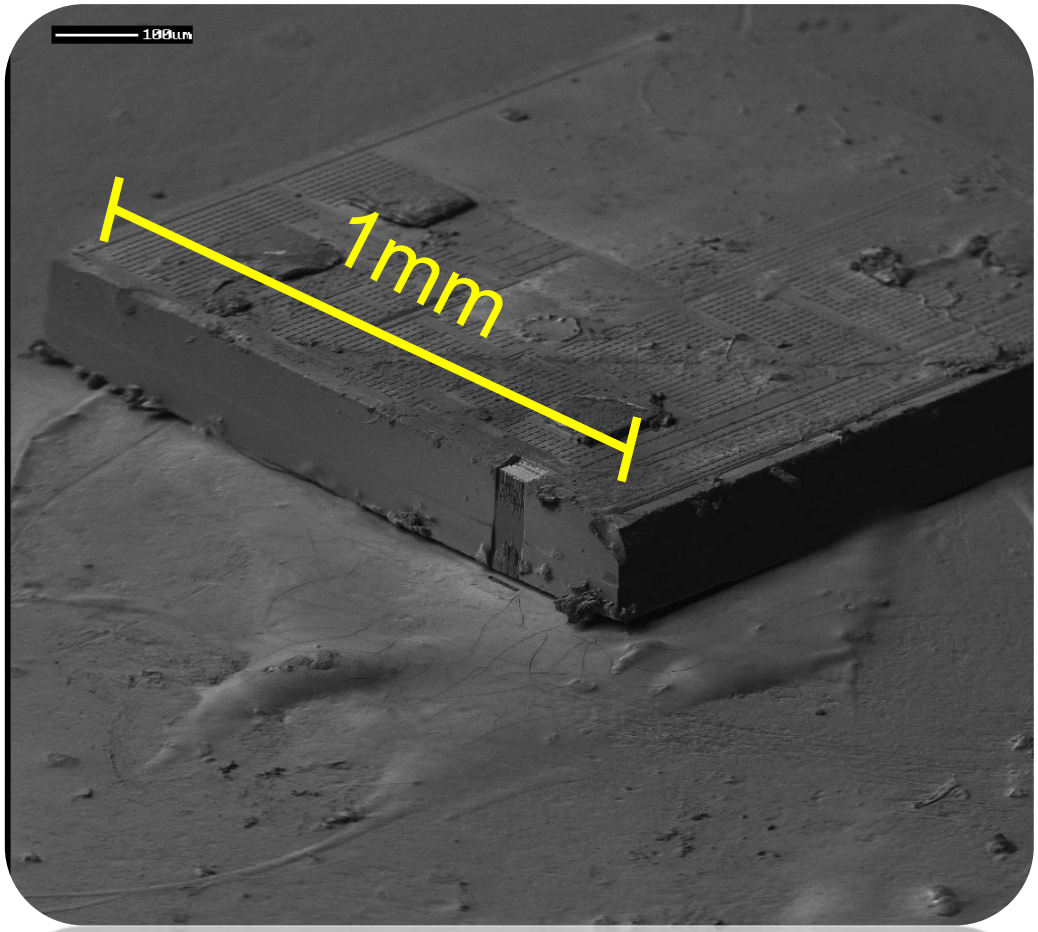
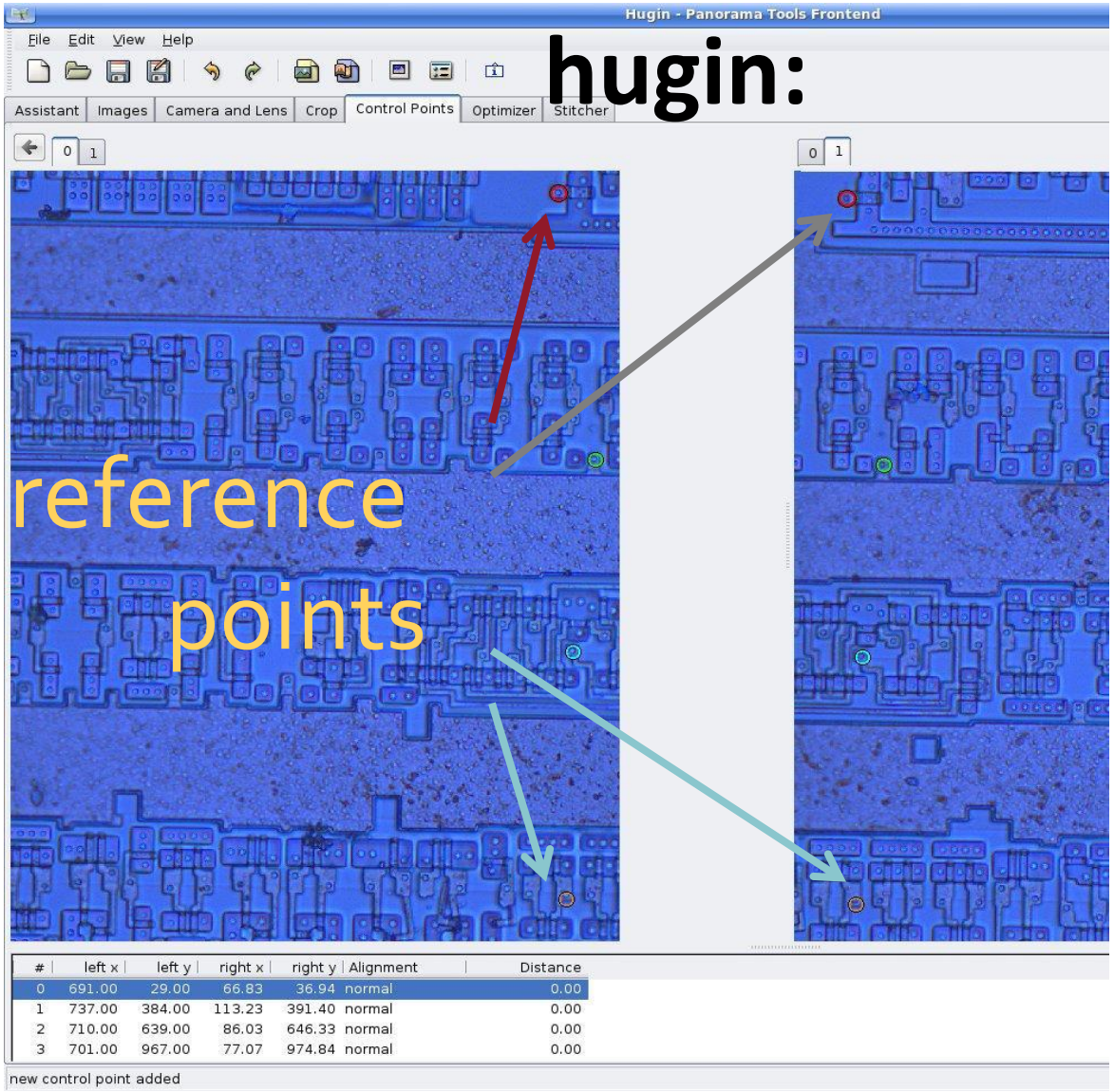


Image tiles are stitched prior to analysis

- Stitch many 100x100µm images
- Previous tool of choice: hugin
- Borrowed from panorama photography



New Image Stitching tool streamlines image tiling

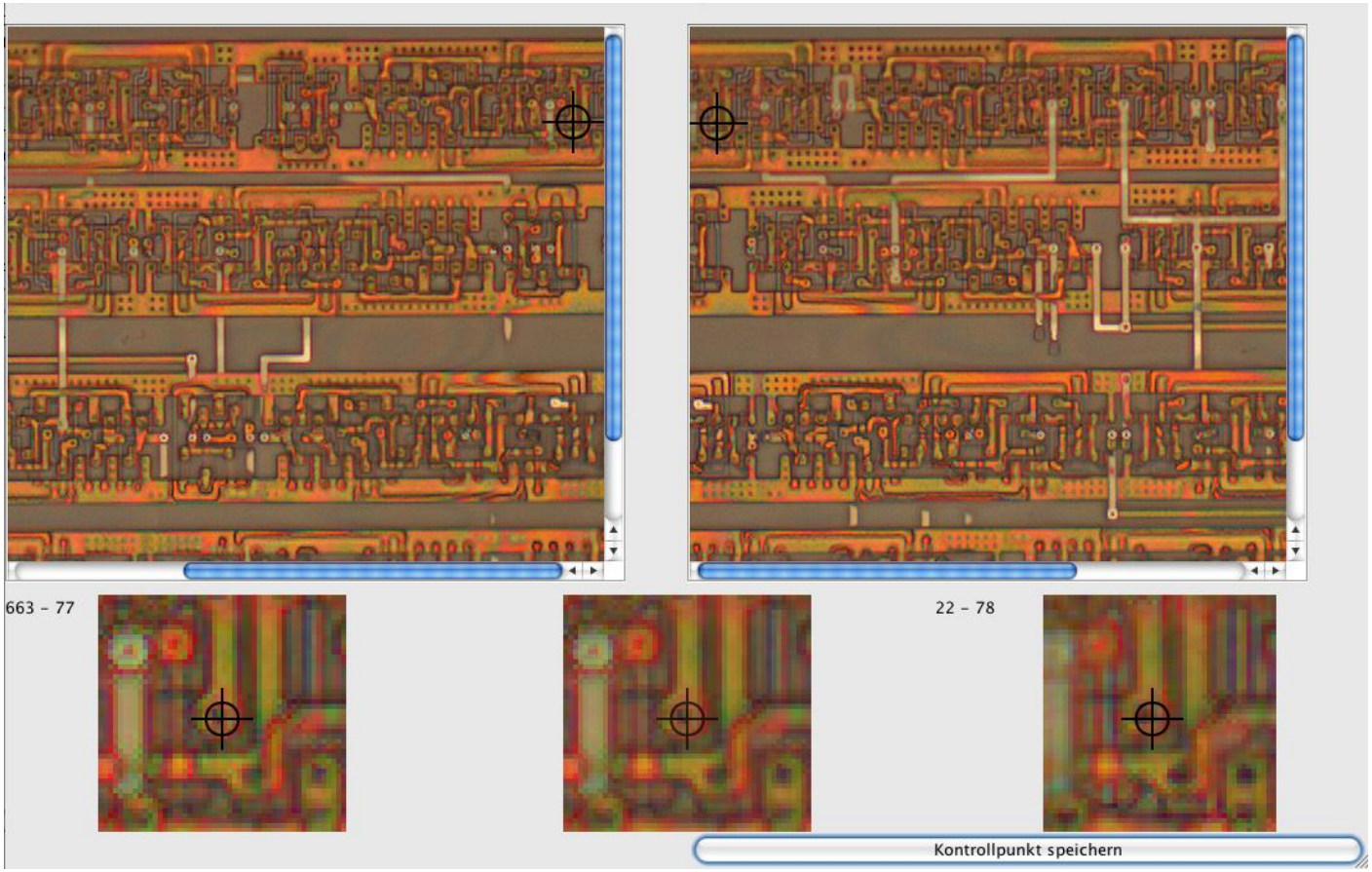
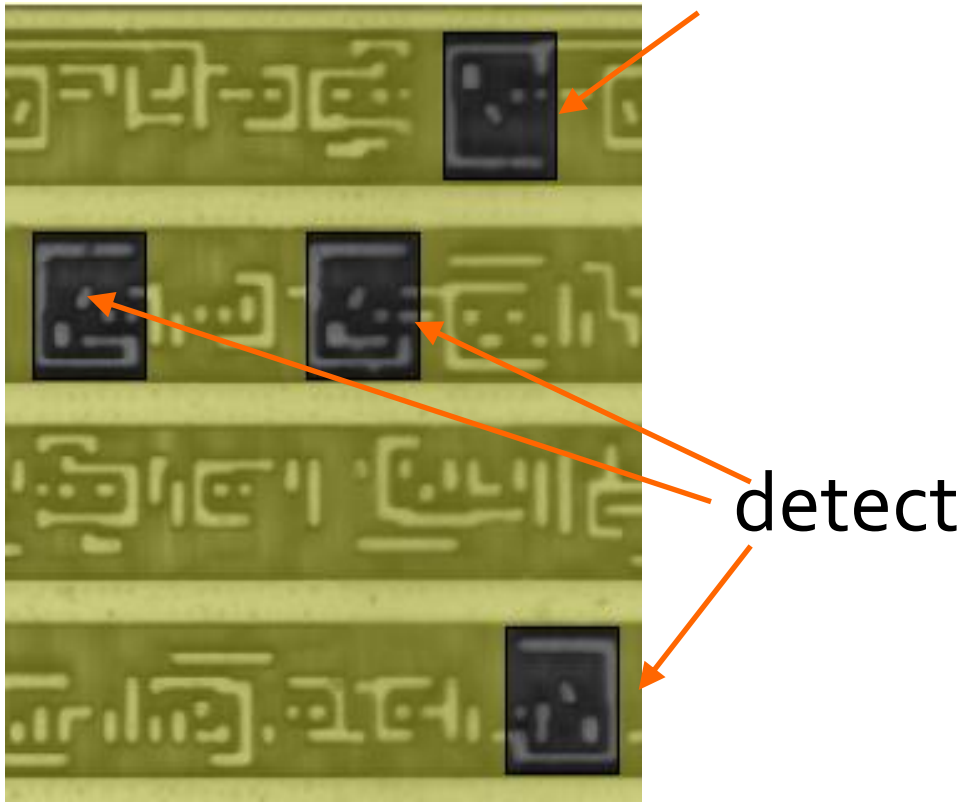


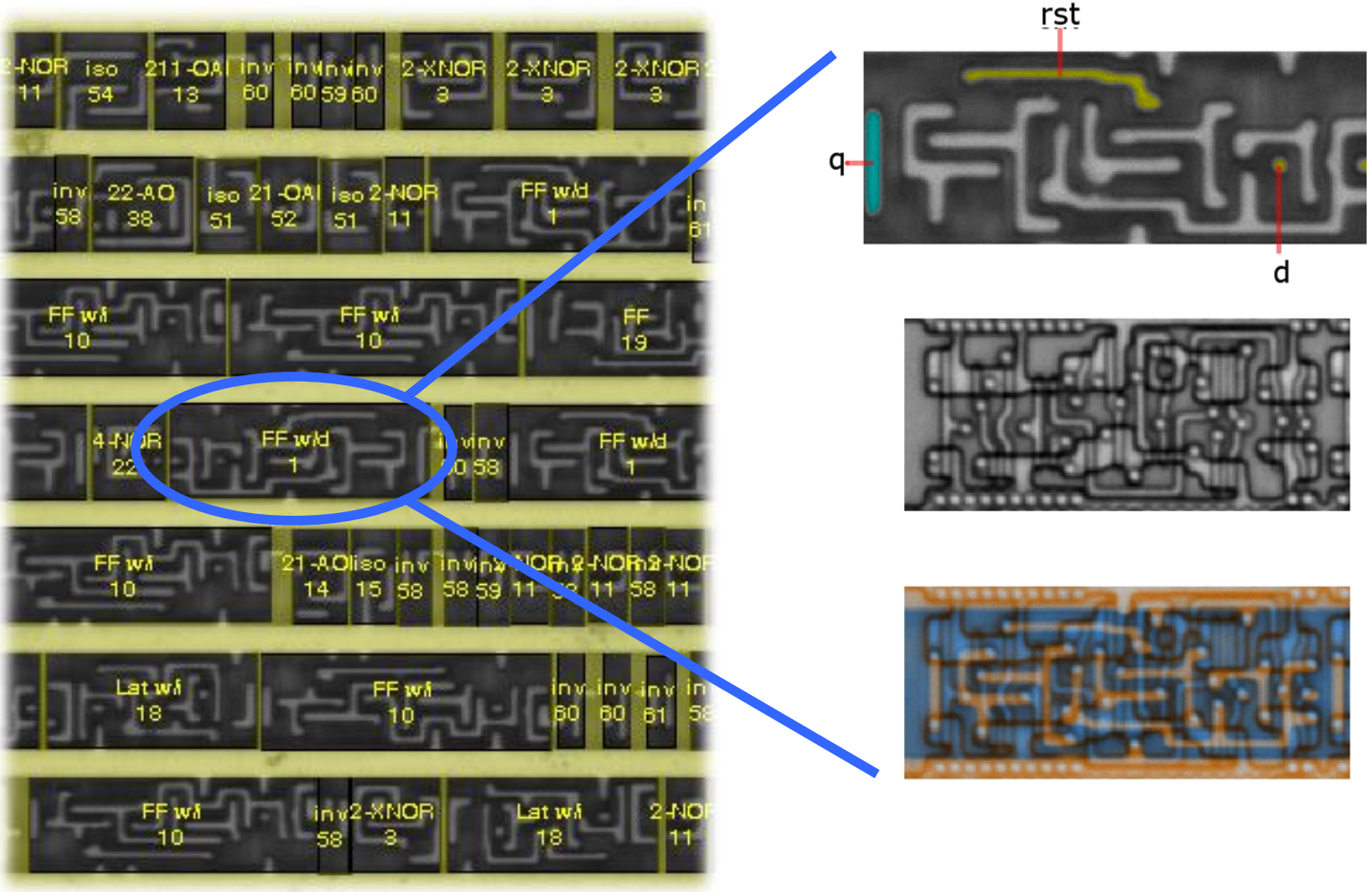
Image Stitching degate.zfch.de/HAR2009/

Silicon circuits are highly structured and hence easy to parse

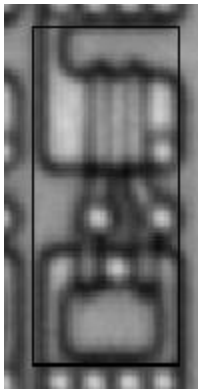
- Logic cells are picked form a library
- Libraries contain a few dozen types of gates
- Detection automated (template matching in Degate)



Automated detection generates map of logic gates



Logic gates implement small binary functions that are easy to recognize



2-NAND Mifare

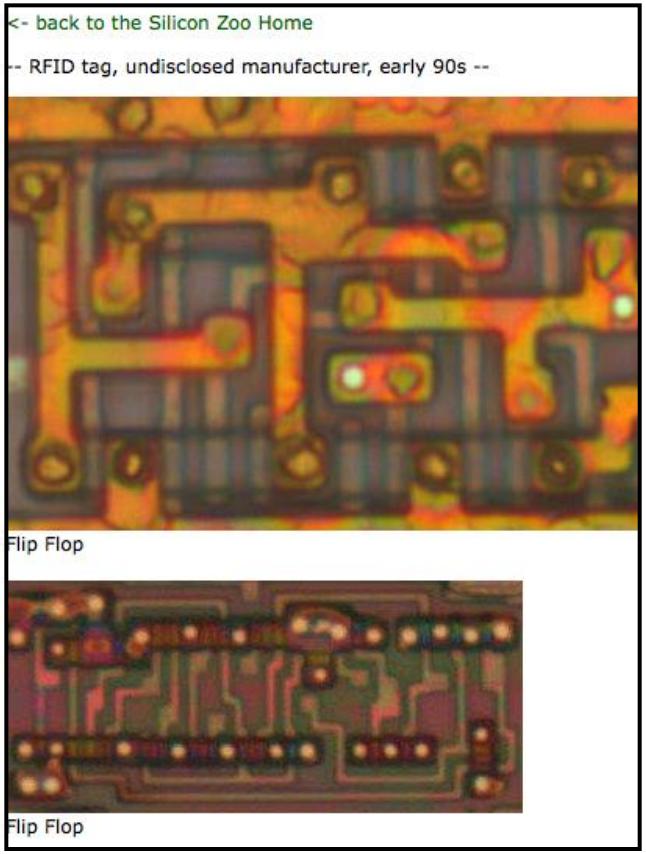
2-NAND Legic

2-NAND DECT

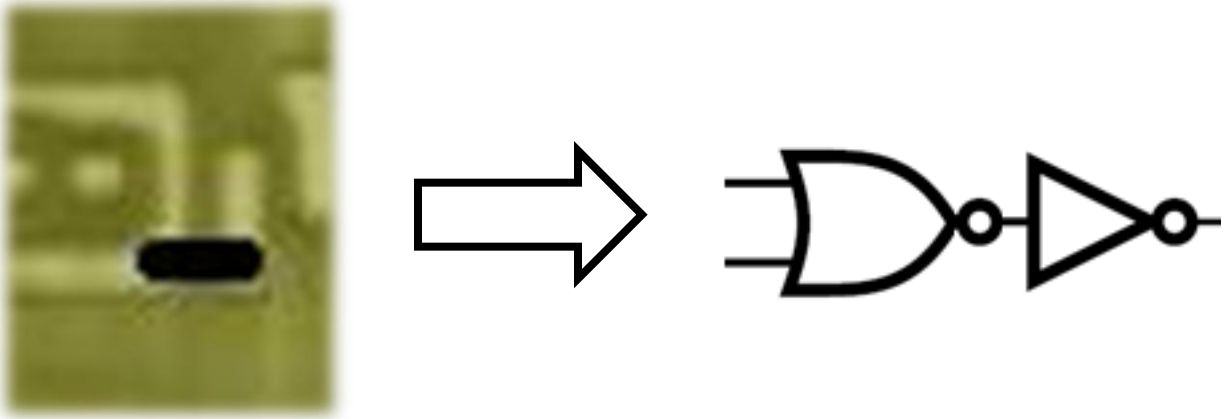
The mapping of common gates to functions is found online

www.siliconzoo.org

- Collection of logic cells
- Free to everyone for study, comparison, and reverse-engineering of silicon chips
- Zoo wants to grow—send your chip images!

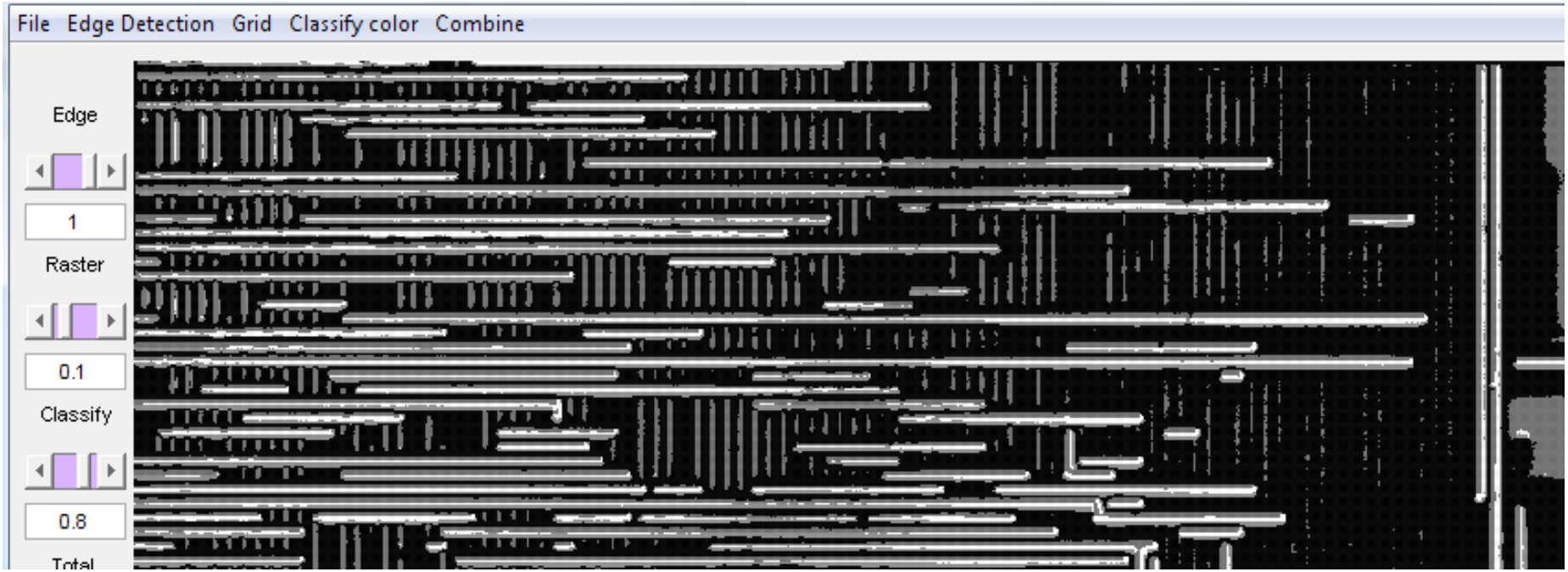


Finally, metal connections are traced to complete circuit description



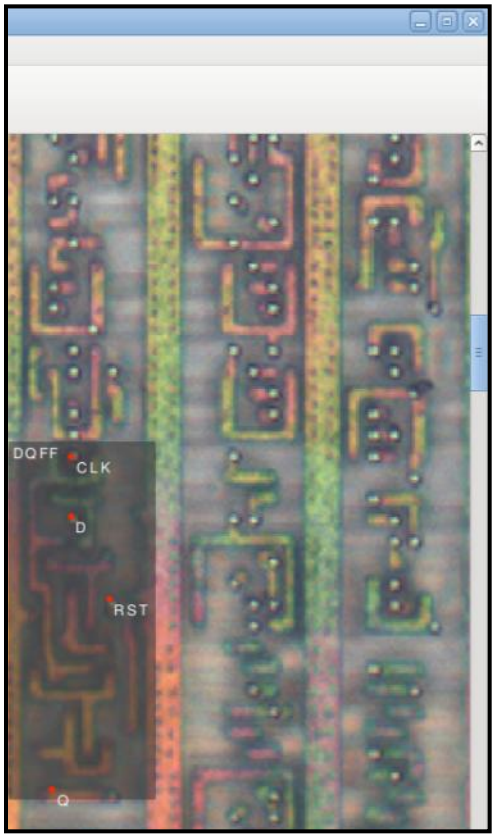
- Mifare: 1500 connections for Crypto-1
- Legic: 2000 connections for Legic Prime
- Manually tracing connections:
  Tedious, time consuming
- Tracing automated (soon to be part of Degate)

Metal tracing is a challenging computer vision problem



- Current implementation overlays results of several filter for most accurate tracking
- MATLAB scripts being ported to Degate

Demo: Degate template matching

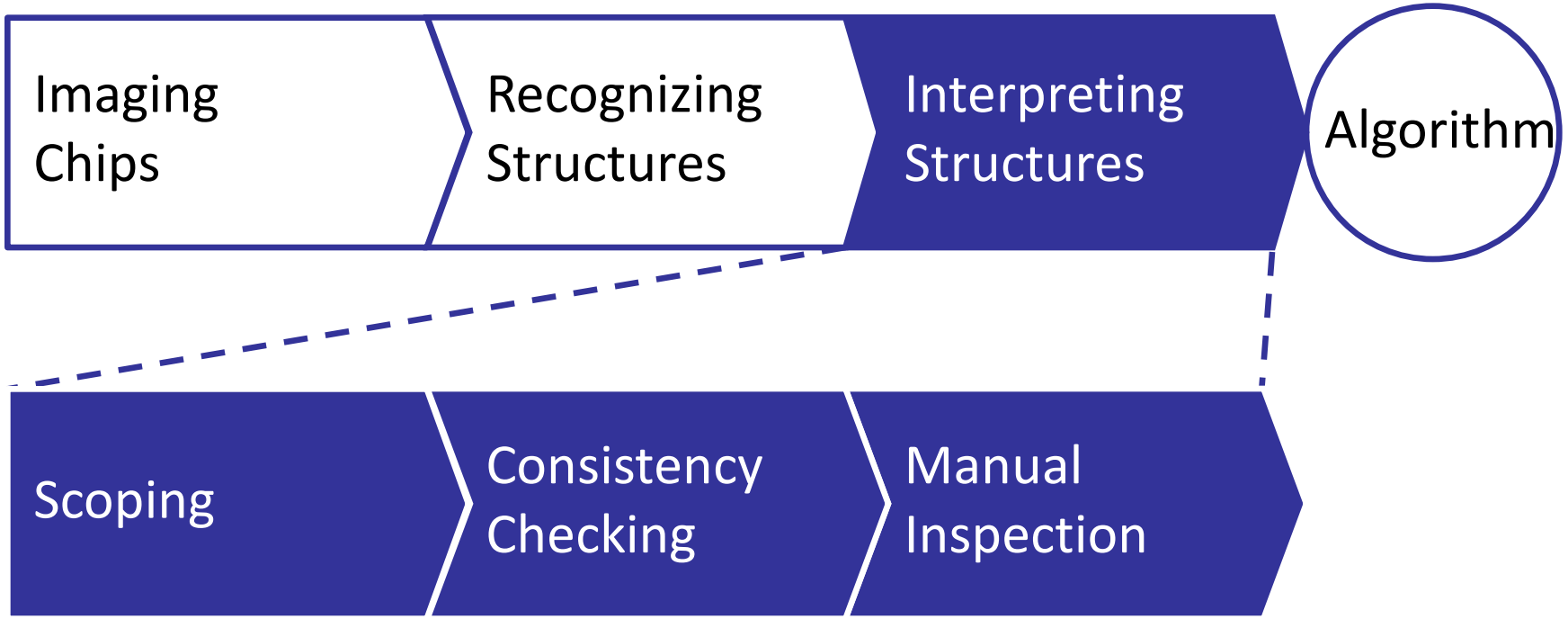


degate.zfch.de

degate

- Author: Martin Schobert <nitram@berlin.ccc.de>
- Released as open source under GPL

Revealing algorithms from netlists still requires design knowledge

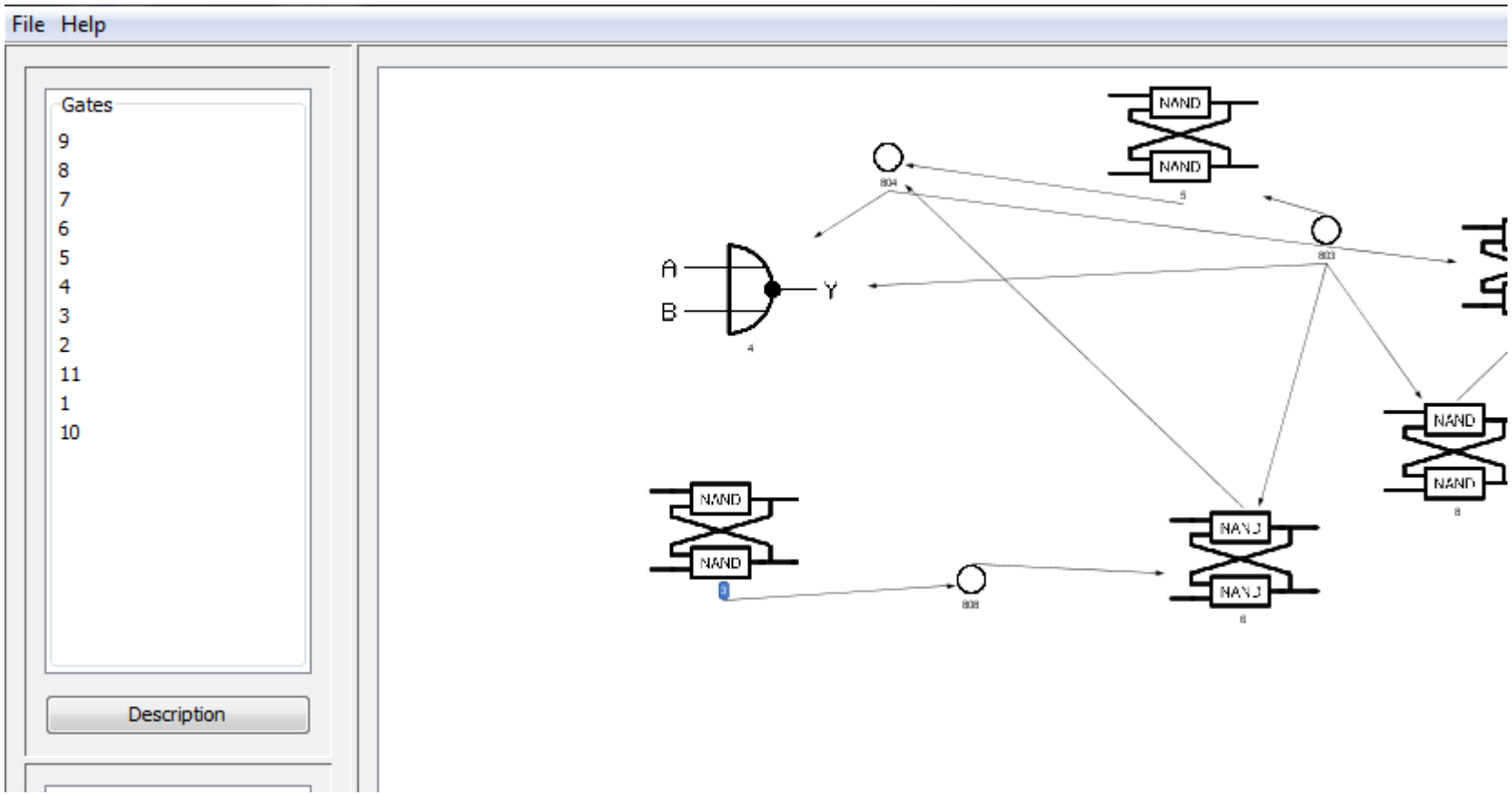


- Crypto: find XORs
- Secret keys: buses, latches

- Electrical consistency
- Logical consistency

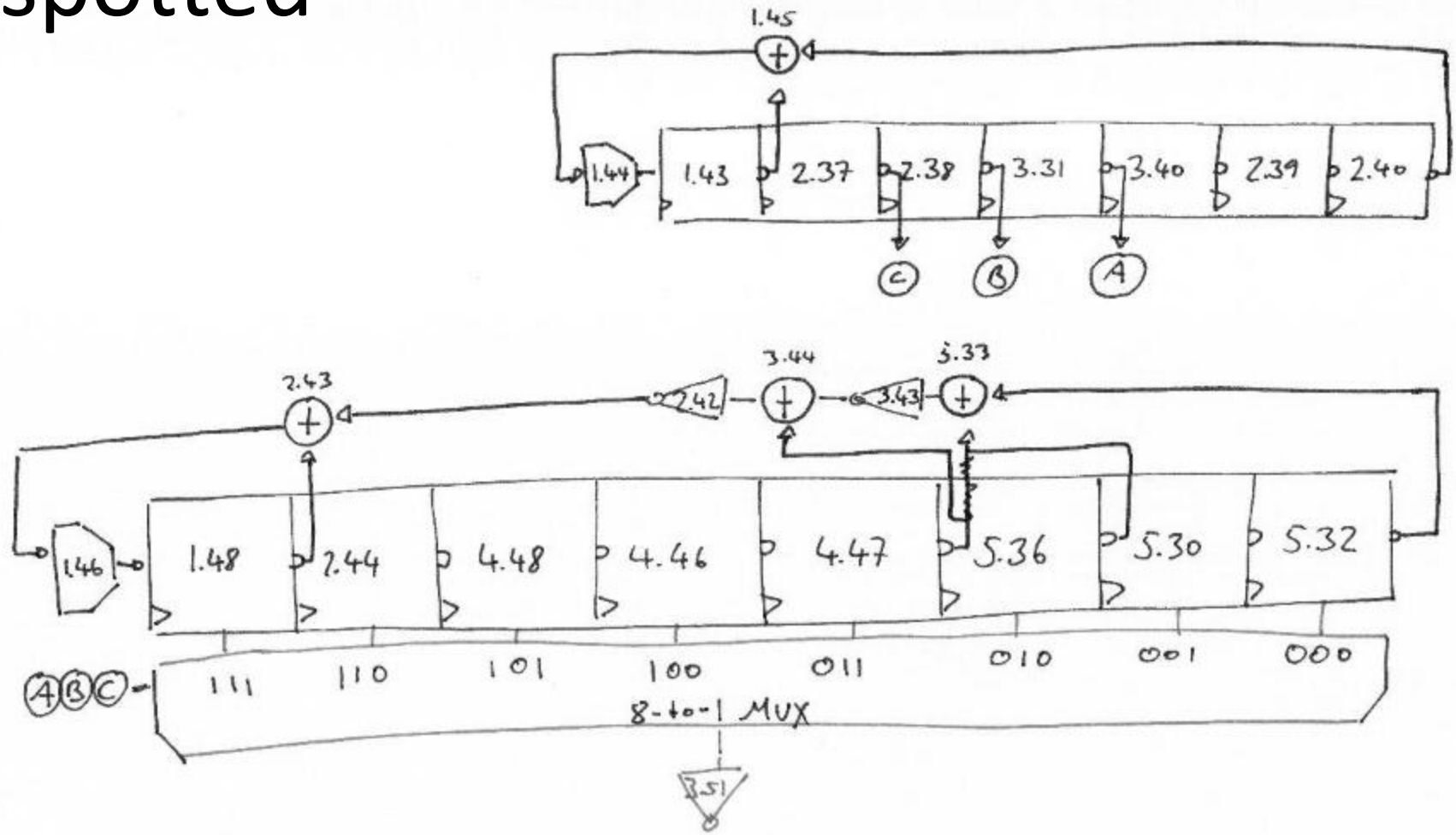
- Group gates into functio-nal units

GateViewer significantly speeds up manual reversing steps

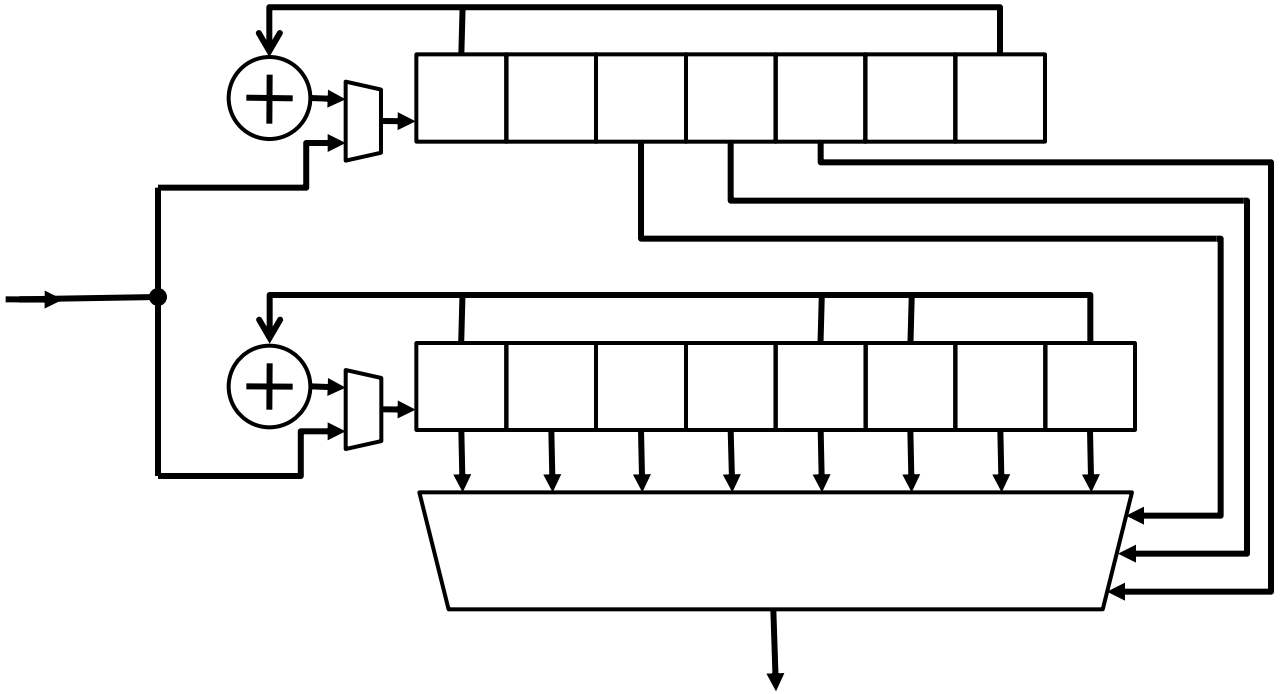


GateViewer degate.zfch.de/HAR2009/

Cryptographic structures are easily spotted



Weak cipher example: Legic Prime



Complete Legic Prime netlist available upon request.

Revealing cryptographic ciphers often breaks their security assumptions

- Cryptographic ciphers revealed and identified as weak …
  - NXP Mifare Crypto-1
  - NXP Hitag2
  - Legic Prime

- … or as potentially weak
  - DECT DSC
  - Atmel CryptoMemory; CryptoRF

Lesson Learned: Hack more silicon.

- Security assumptions in hardware never hold universally true
- Algorithms must be documented for independent security reviews
- Process of revealing algorithms from silicon chips is mostly streamlined

Deep silicon analysis must become mandatory for trusted chips

Lots of project ideas remain …

The *silicon disassember* should be further automated and extended to more application domains:

- Automate imaging
  - Low-cost stepper (any Reprap/Makerbot folks here?)
- Extend Degate
  - Support for full-custom chips (Retro comp. fans?)
  - Tight integration of consistency checks (EE geeks?)

We are looking for interns as well as professional support for industry projects.

Questions?

Degate	degate.zfch.de
Silicon Zoo	siliconzoo.org
Image Stitching, GateViewer, Slides	degate.zfch.de/HAR2009/

Karsten Nohl	<nohl@virginia.edu>
Starbug	<starbug@ccc.de>

Many Thanks to Martin Schobert, Christin Schulz, Stefan Skillen, Daniel Wittekind and Sven Kaden !