

The Last HOPE  
Karsten Nohl—Univ. of Virginia



**The (Im)possibility of  
Hardware Obfuscation**

# Motivation

- ◆ Most security systems use cryptography
  - ◆ Too many use proprietary ciphers
  - ◆ Many are weak, but secret
- ◆ We find cipher implementations from silicon
  - ◆ Cheap approach, no crypto knowledge required
  - ◆ We want to enable you to do the same

“No more weak ciphers. No more paranoia.”

Sean O’Neil

**Motivating example: RFID**

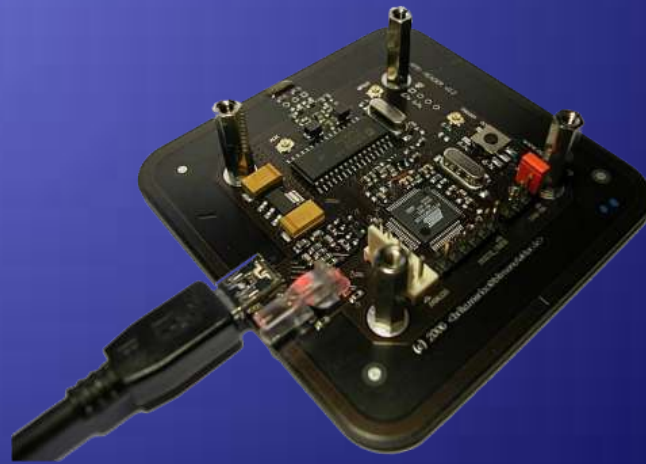
# RFID tags

- ◆ Radio Frequency IDentification
- ◆ Tiny computer chips
- ◆ Passively Powered



# Our Project (Starbug, Henryk Plötz, me)

We reverse-engineered the Mifare crypto and evaluated its security



# Reverse-Engineering

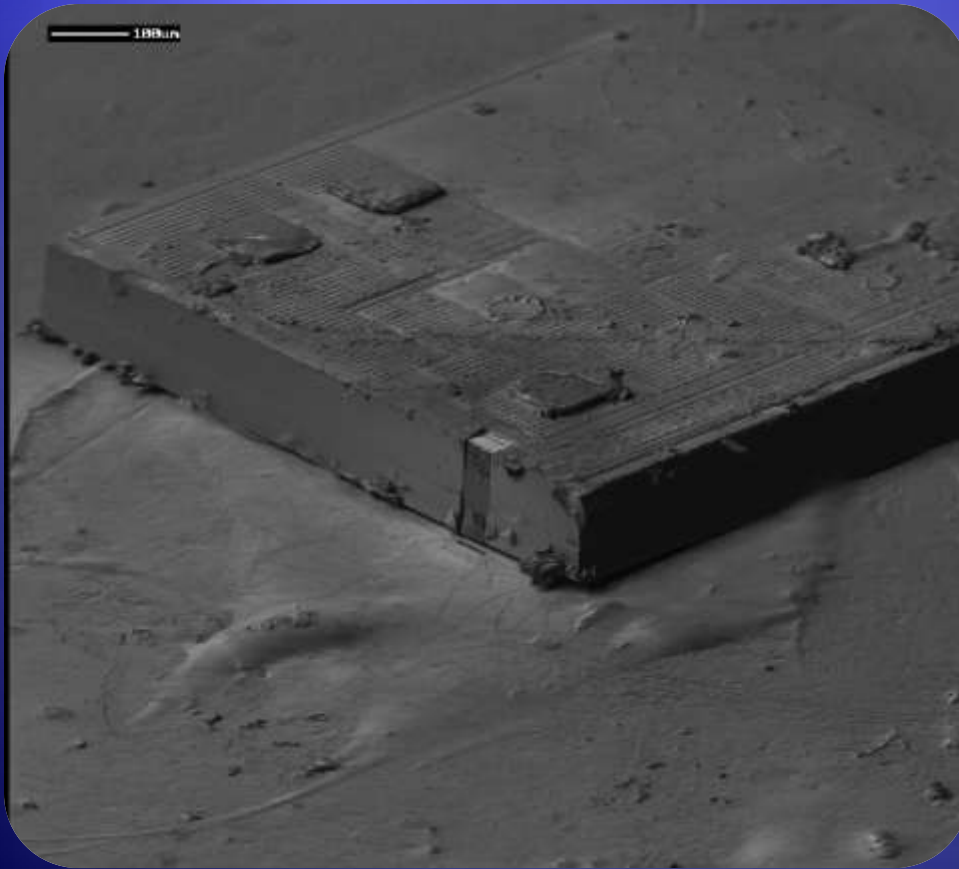
# Obtaining Chips



- ◆ Chemically extract chips:
  - ◆ Acetone
  - ◆ Fuming nitric acid
- ◆ Shortcut: buy blank chips!



# Mifare Classic RFID tag

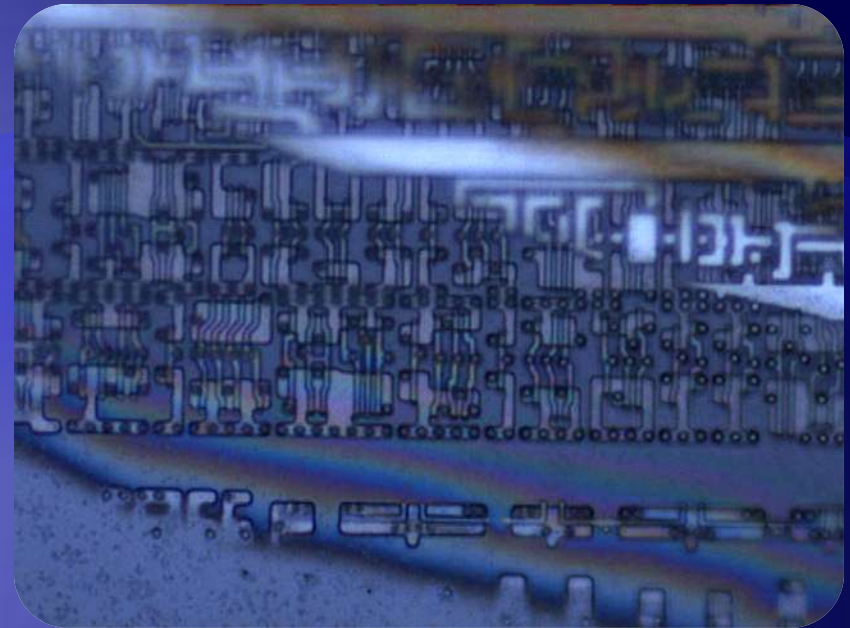




# Polishing

- ◆ Embed chip in plastic
  - ◆ Downside: chip is tilted
- ◆ Automated polishing with machine
  - or—
  - Manually with sand paper
- ◆ “On your kitchen table”

-Starbug

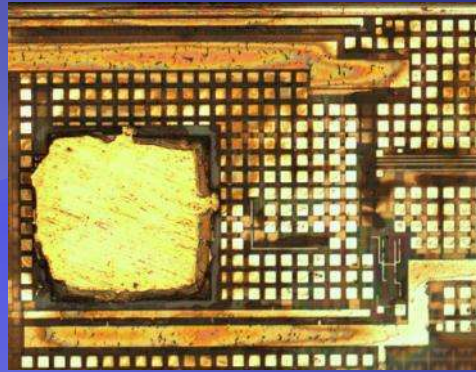


# Imaging Chip

- ◆ Simple optical microscope
  - ◆ 500x magnification
  - ◆ Camera 1 Mpixel
  - ◆ Costs < \$1000, found in most labs
- ◆ Stitching images
  - ◆ Panorama software (hugin)
  - ◆ Each image  $\sim 100 \times 100 \mu\text{m}$
- ◆ Align different layers

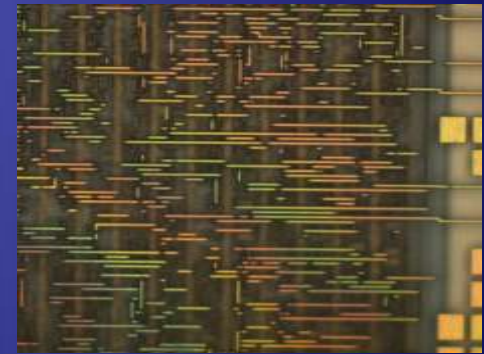
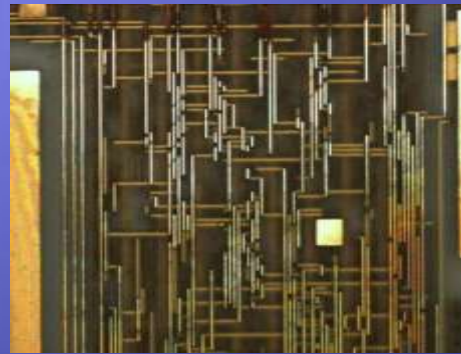
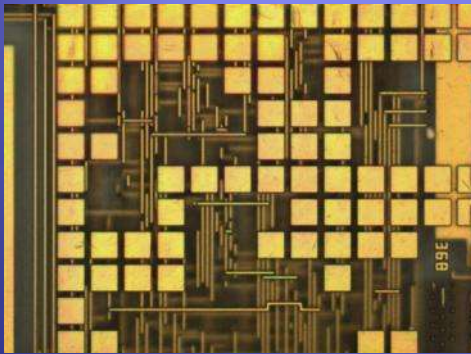


# Chip Layers

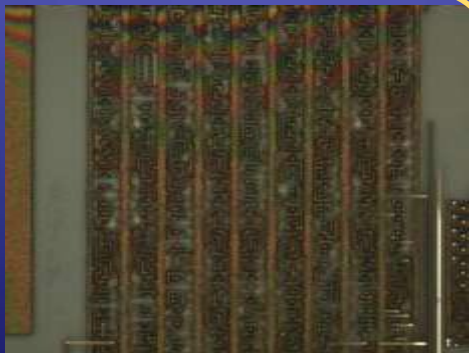


Cover layer

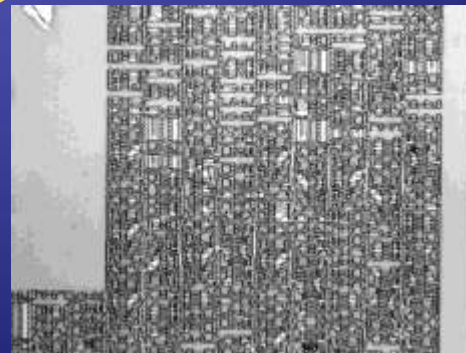
## 3 Interconnection layer



Logic layer

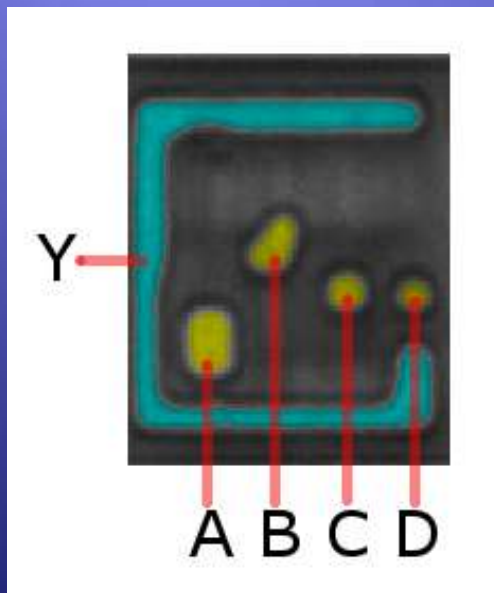


Transistor layer

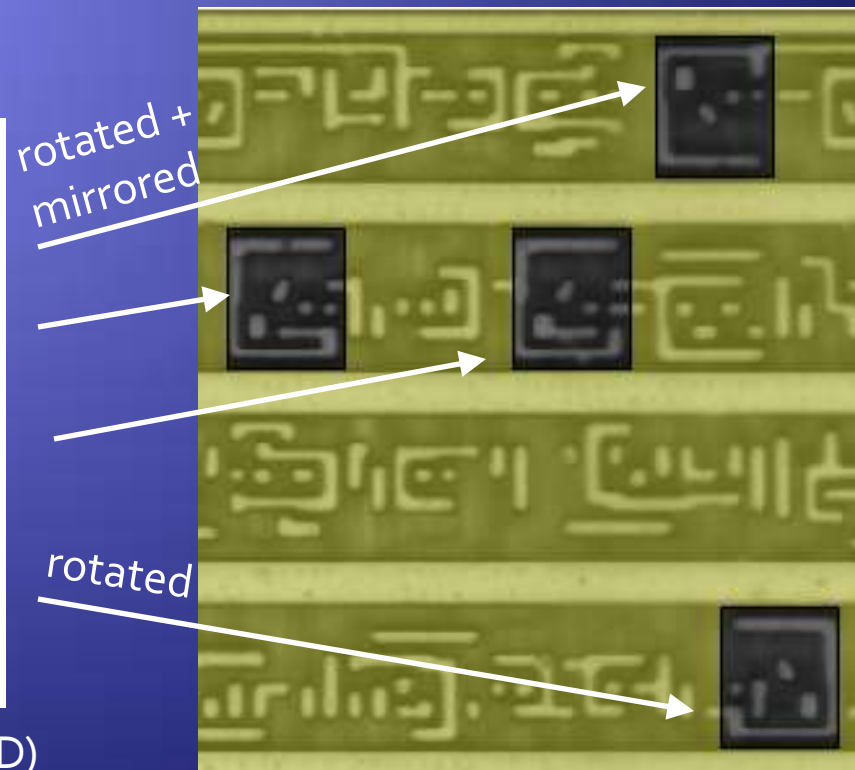


# Logic Cells

- ◆ Chip consists of small cells that perform simple logic functions

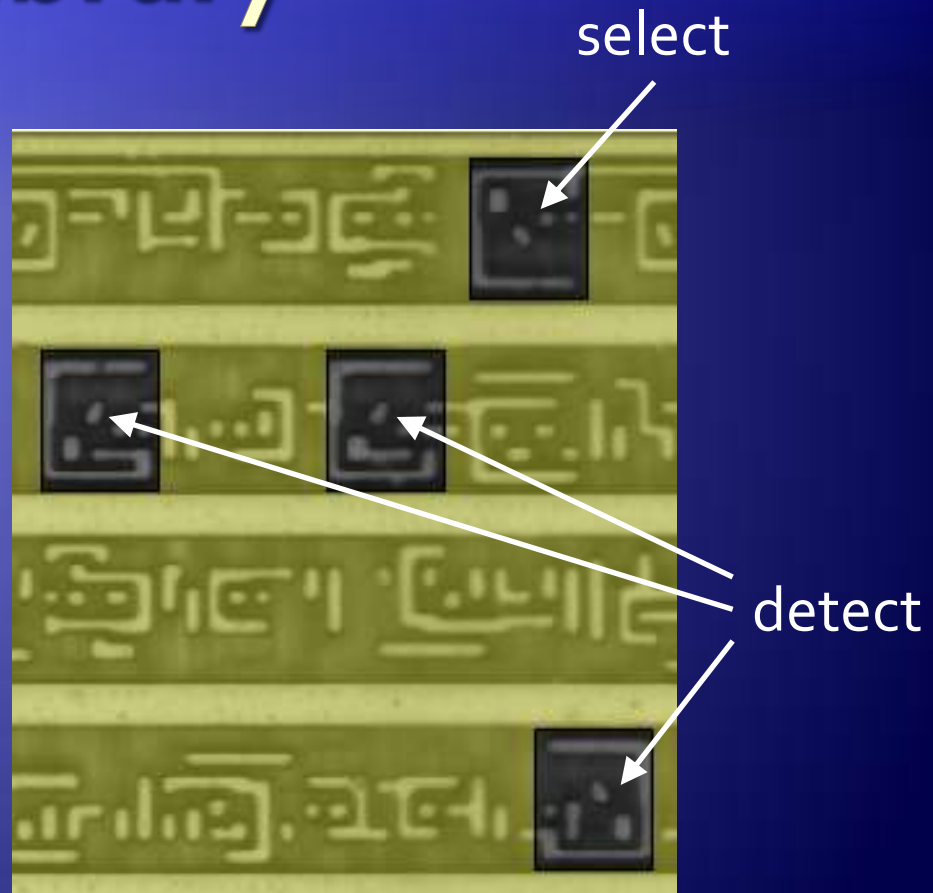


4 NAND:  $Y = \neg(A \& B \& C \& D)$

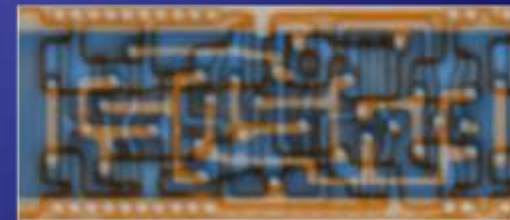
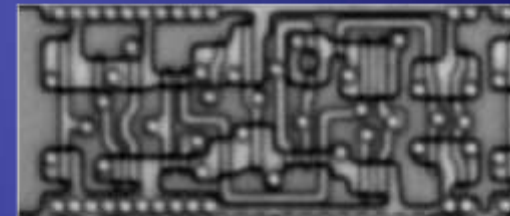
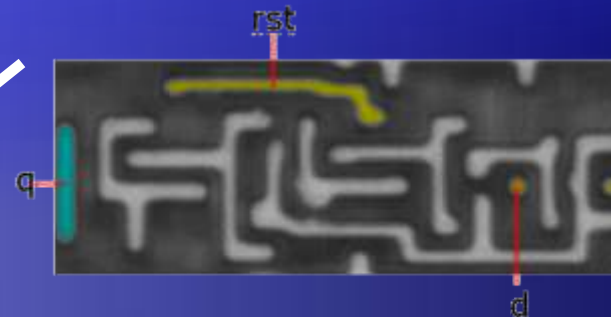


# Standard Cell Library

- ◆ Logic cells are picked from a library
  - ◆ Library contains less than 70 types of gates
  - ◆ Detection can be automated through template matching

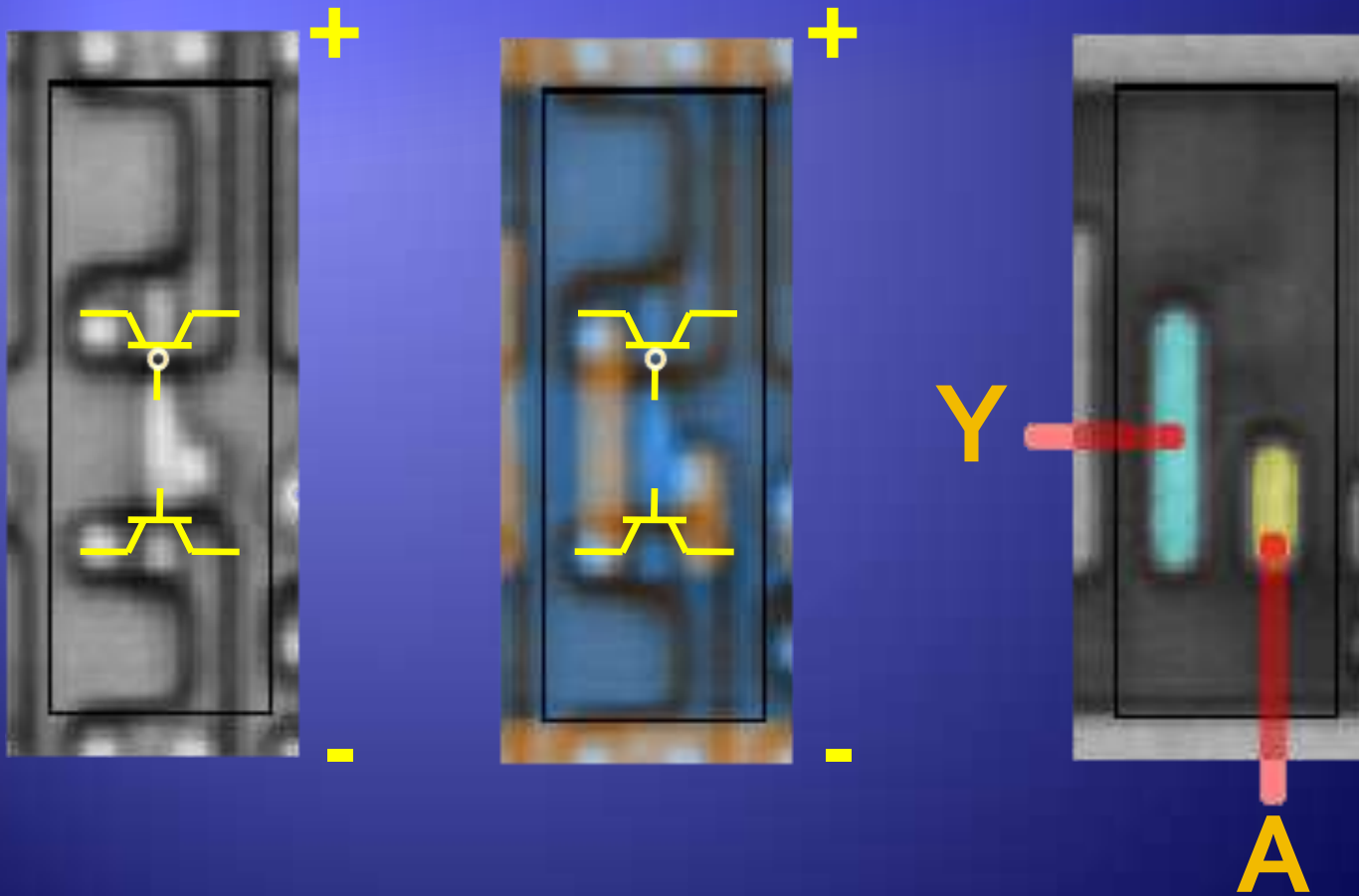


# Automated Logic Cell Detection

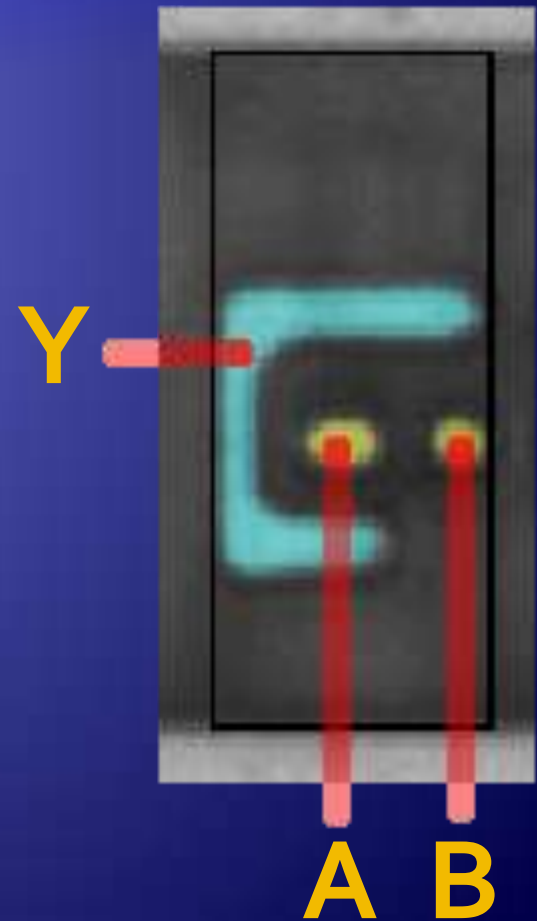


Next: Finding the function of each cell type.

# Logic Gates – Inverter



# Logic Gates – 2NOR





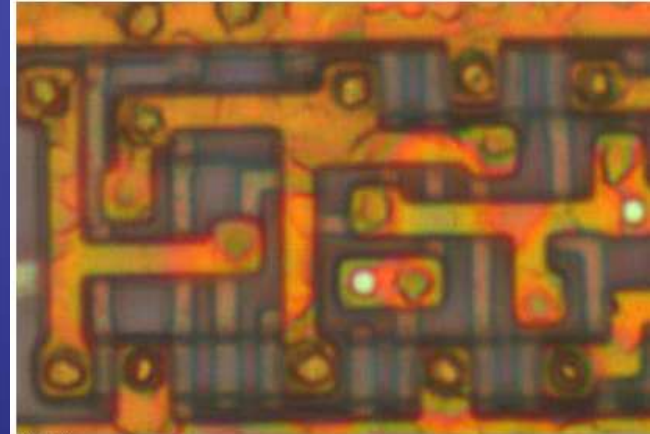
# The Silicon Zoo

[www.siliconzoo.org](http://www.siliconzoo.org)

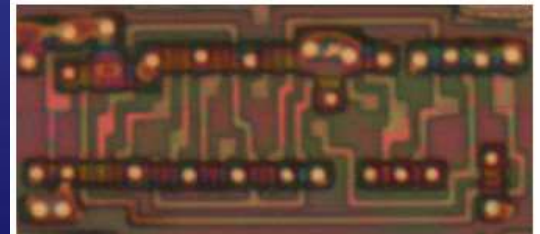
- ◆ Collection of logic cells
- ◆ Free to everyone for study, comparison, and reverse-engineering of silicon chips
- ◆ Zoo wants to grow—send your chip images!

<- back to the Silicon Zoo Home

-- RFID tag, undisclosed manufacturer, early 90s --



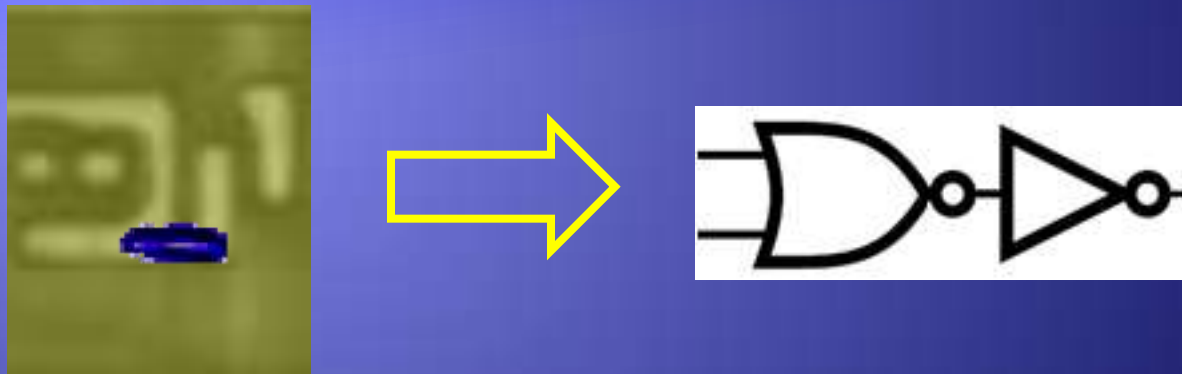
Flip Flop



Flip Flop

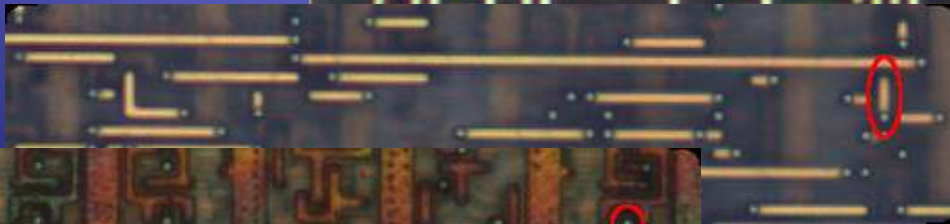
# Logic Gates Interconnect

- ◆ Connections across all layers

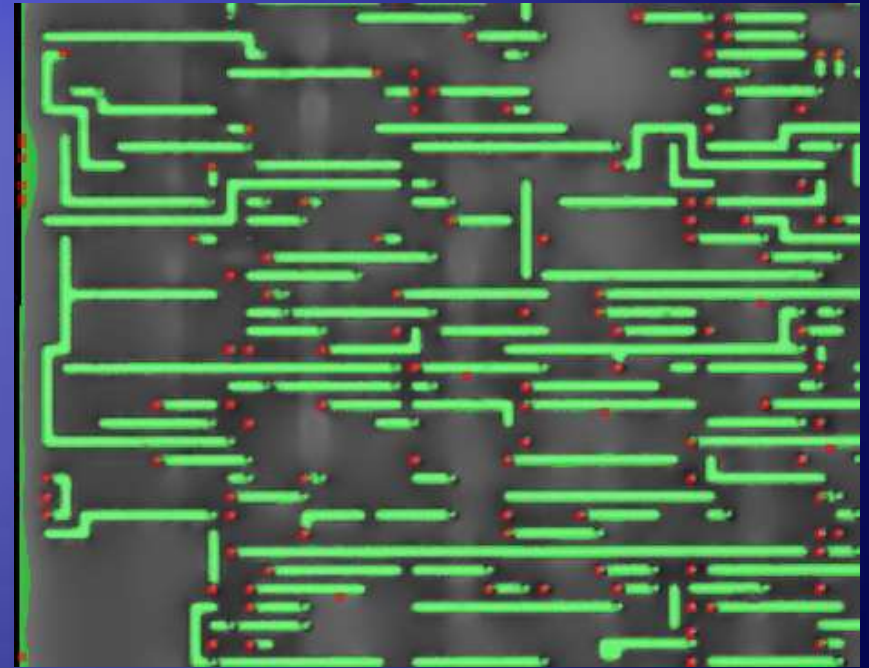




- ◆ Traced 1500 (!) connections manually
  - ◆ Tedious, time consuming
  - ◆ Error-prone (but errors easily spottable)
  - ◆ Tracing completely automated by now

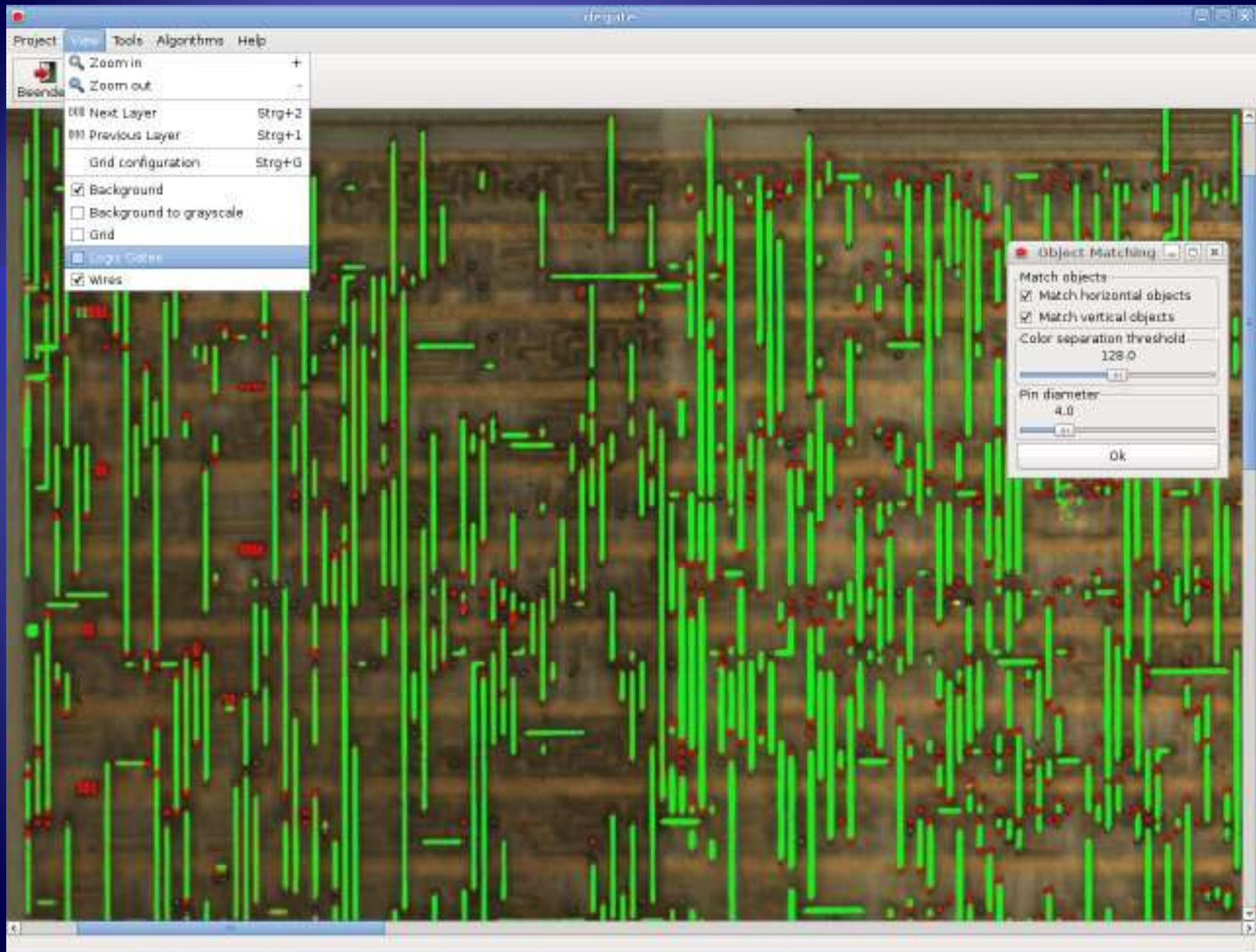
# Tracing Connections



# Automated Tracing



-  Metal wire
-  Intra-layer via

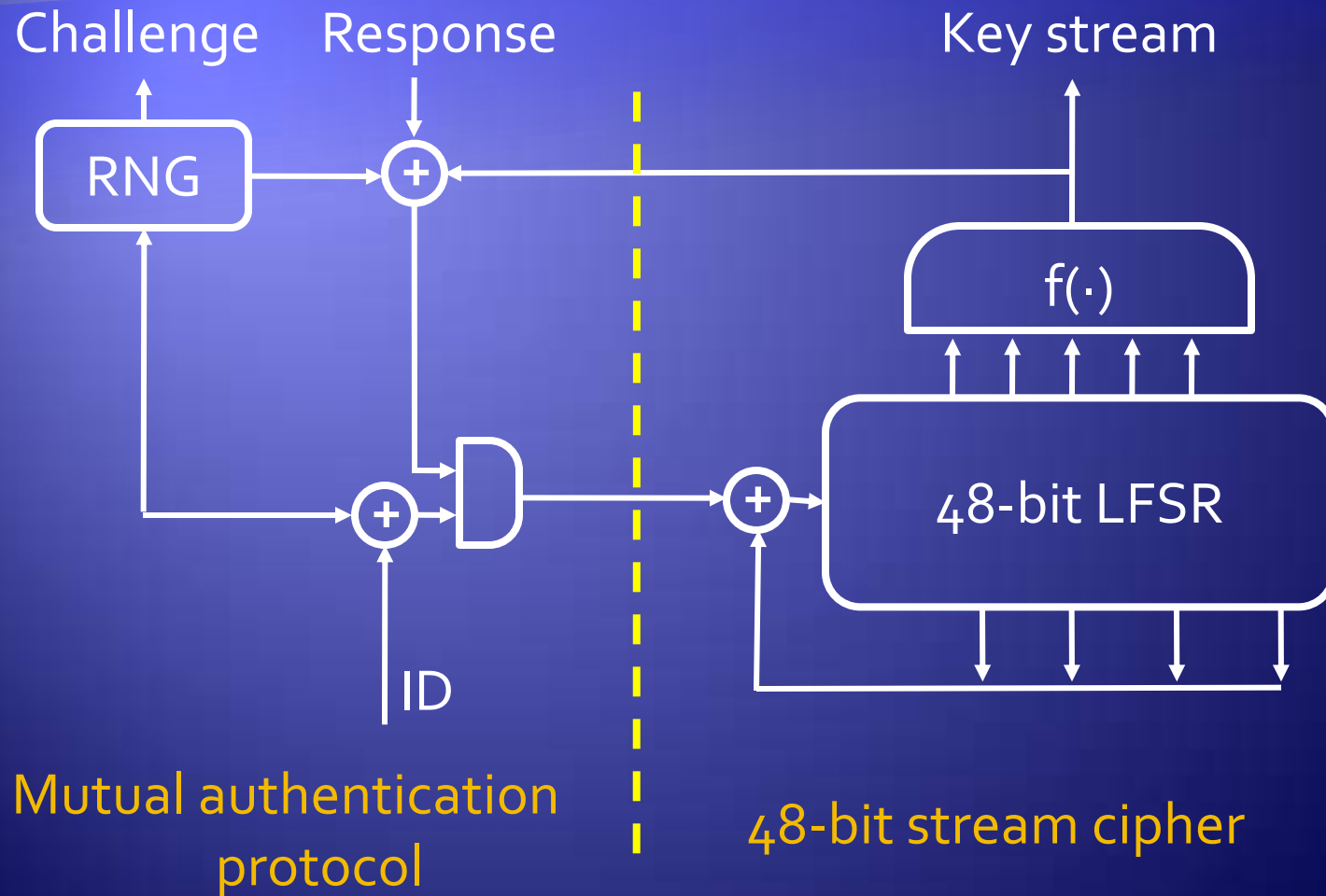


# Countermeasures

- ◆ Obfuscated placing and wiring of logic cells
  - ◆ May defeat human inspection, but not automated tools
- ◆ Dummy cells
  - ◆ Makes reversing harder, but not impossible
- ◆ Large chips
  - ◆ Huge effort, huge rewards?
- ◆ Self-destructive chips?
  - ◆ May protect secret keys, not secret algorithms

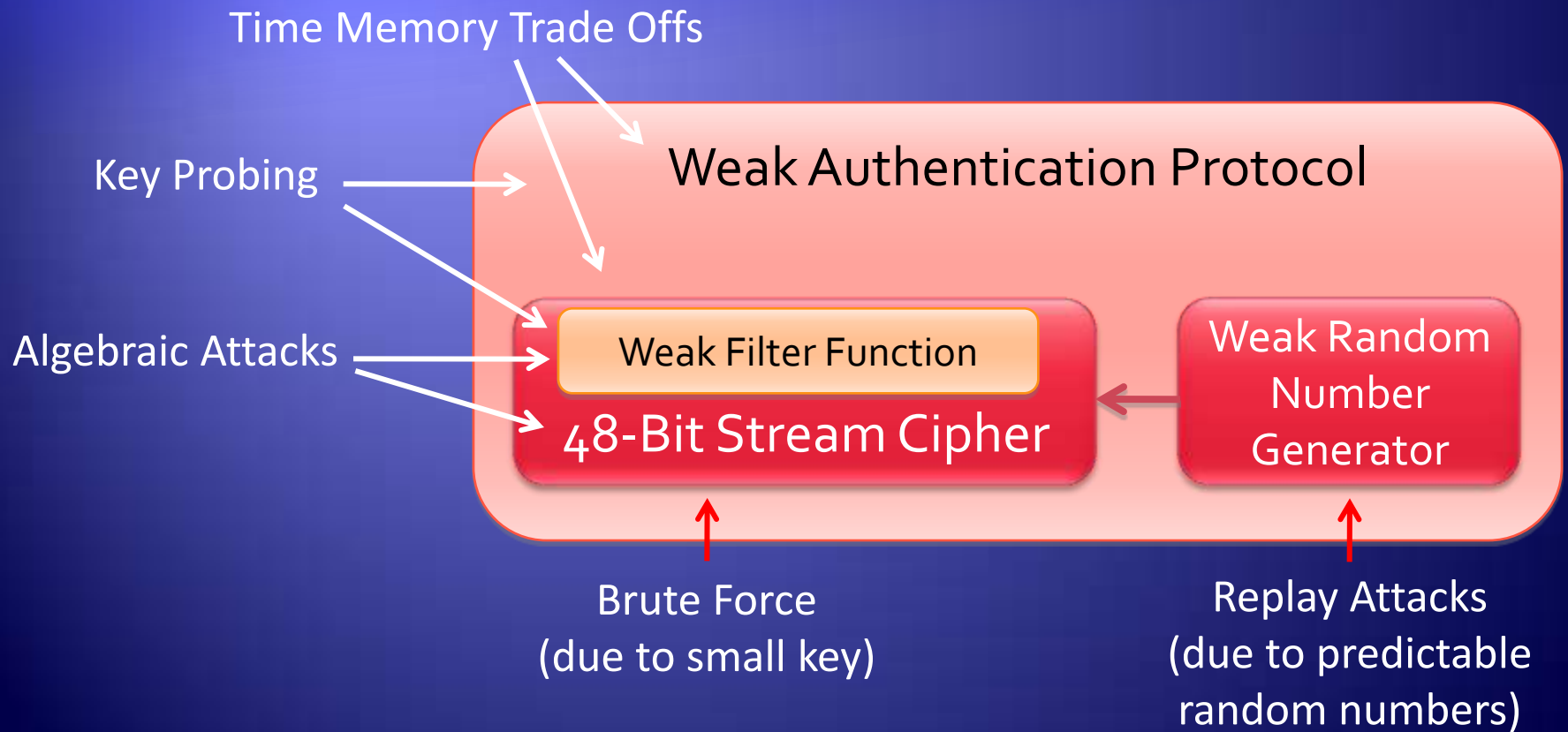
**Result: Mifare Classic's Crypto**

# Mifare Crypto-1





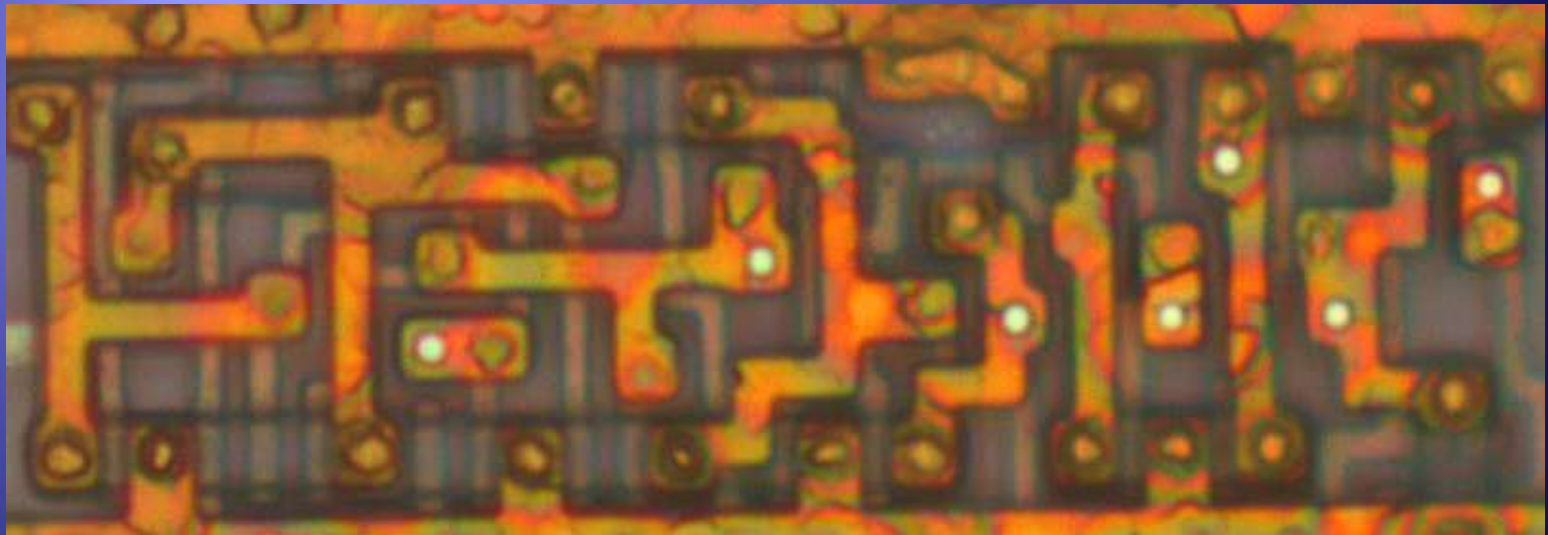
# Mifare Classic Weaknesses



# Lessons Learned

- ◆ Reverse-Engineering is possible
  - ◆ you should try! (I'll help)
  - ◆ Easy targets: small chips with proprietary crypto
  - ◆ Obfuscation help very little against automated circuit reconstruction
- ◆ Obscurity adds security only in the short-run
  - ◆ Lack of peer-review hurts later

# Questions?



Karsten Nohl  
nohl@virginia.edu

Talk to me about your  
reverse-engineering ideas!