BlackHat '08

Karsten Nohl—Univ. of Virginia

MIFARE— Little Security, despite Obscurity

Motivation

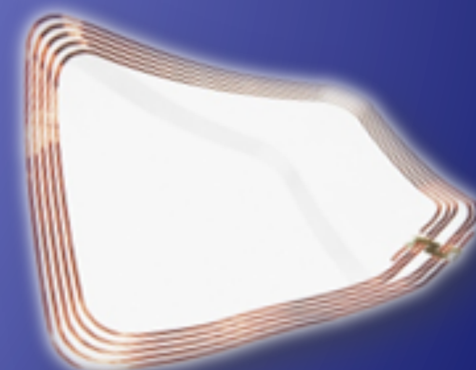
- Most security systems use cryptography
  - Too many use proprietary ciphers
  - Many are weak, but secret
- We find cipher implementations from silicon
  - Cheap approach, no crypto knowledge required
  - We want to enable you to do the same

"No more weak ciphers. No more paranoia."
Sean O'Neil

Motivating example: RFID

RFID tags

- Radio Frequency IDentification
- Tiny computer chips
- Passively Powered

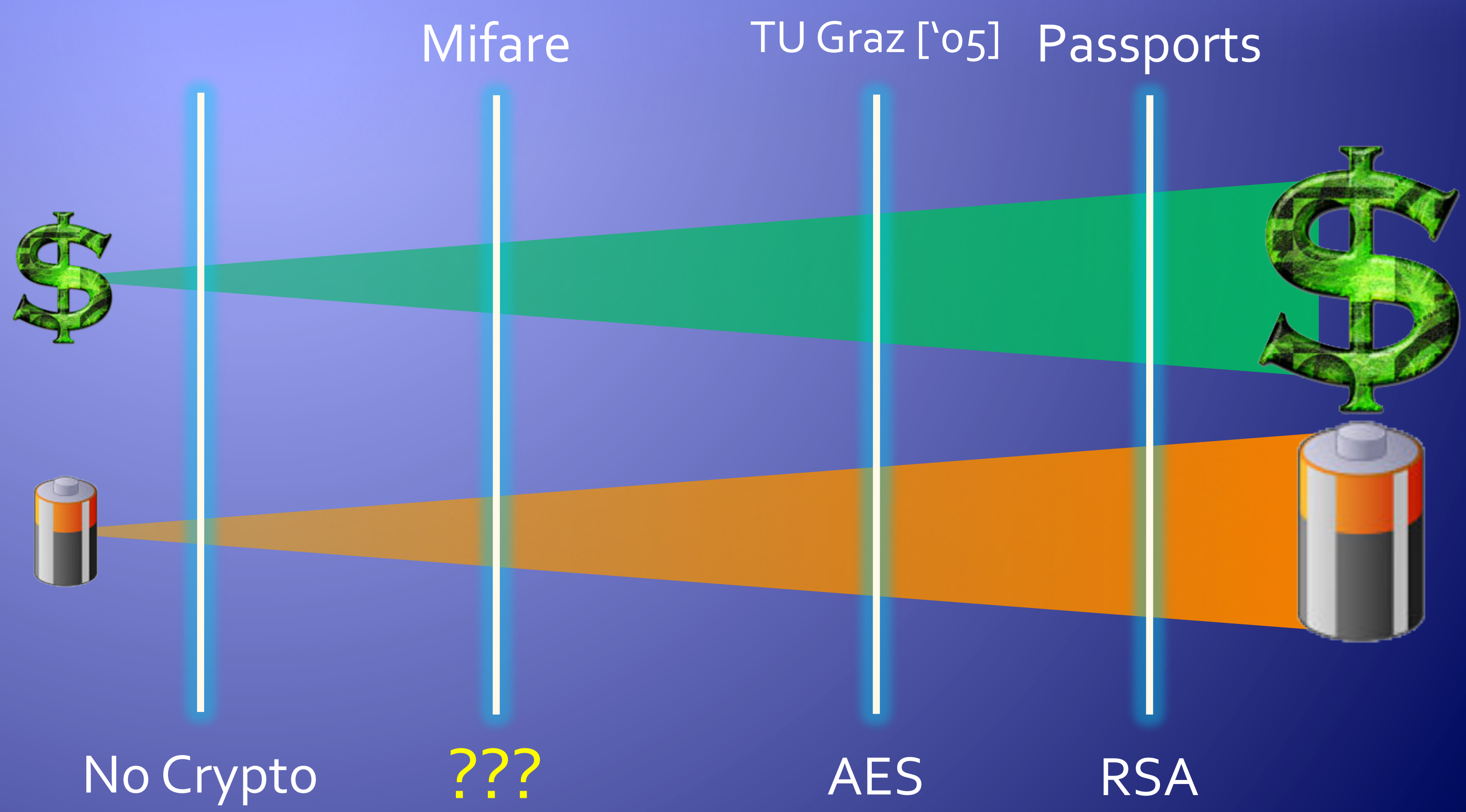


RFID Applications

- RFIDs are becoming ubiquitous
- Integrated in many *security* applications
  - Payment, Access Control
  - Passports, Car Ignition
  - Implants, ...

RFIDs will be *universal identifier*. Might replace passwords, PINs, and fingerprints.

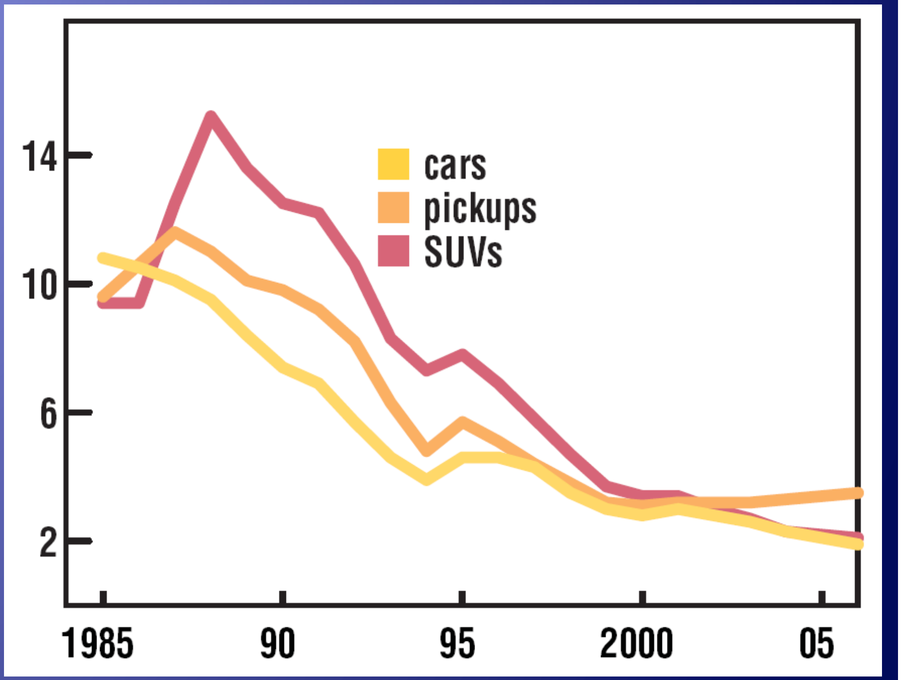
RFID-Crypto Mismatch



Mifare Security

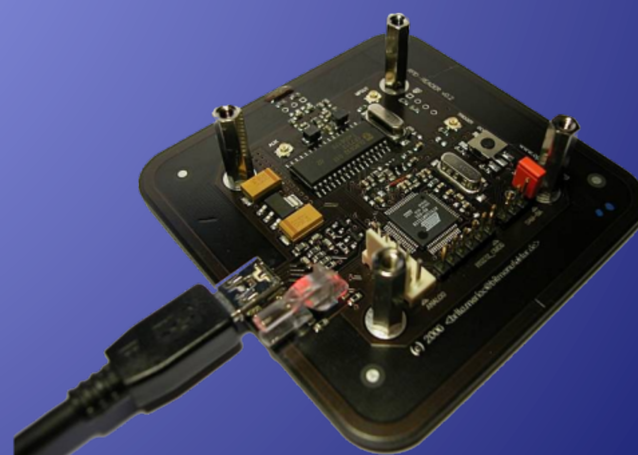
- NXP claimed:
  - “approved authentication”
  - “advanced security levels”
- Stream cipher
- 48 bit key

Car thefts
(source: hldi.org)



Our Project (Starbug, Henryk Plötz, me)

We reverse-engineered the Mifare crypto and evaluated its security

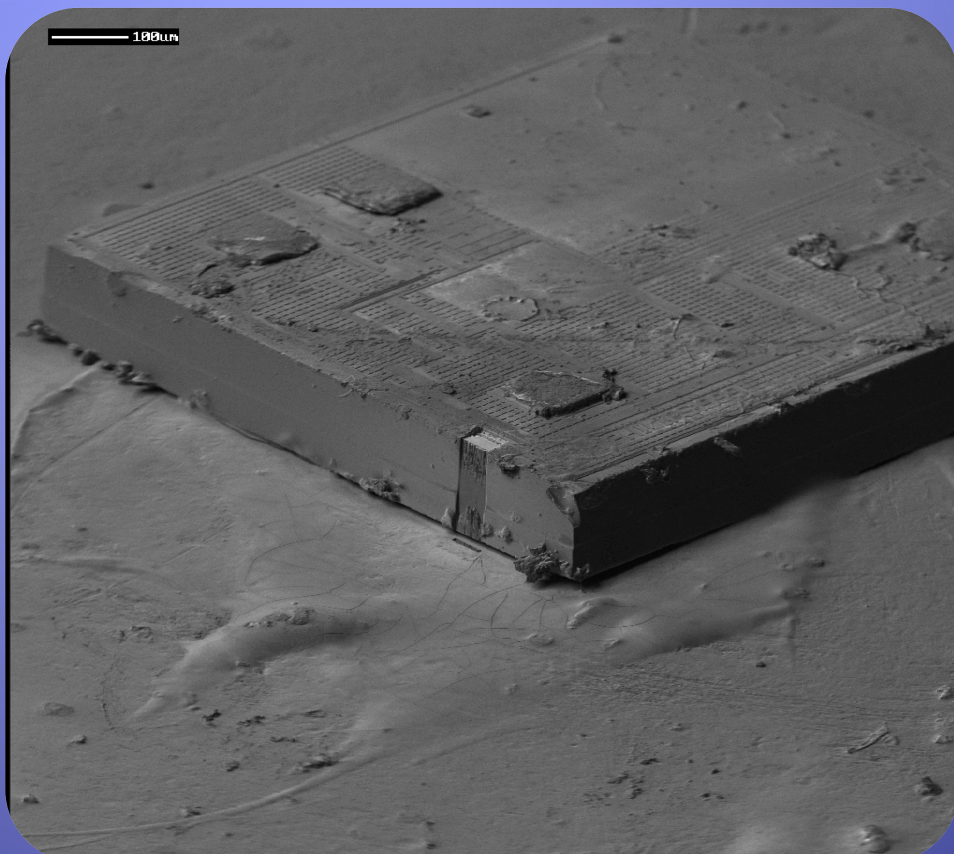


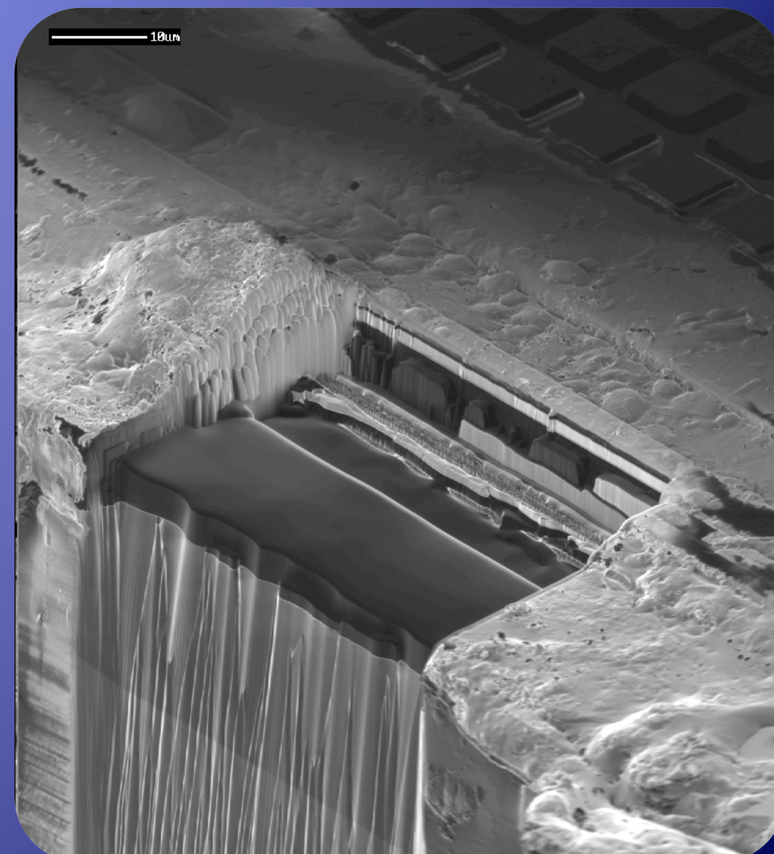
Reverse-Engineering

Obtaining Chips

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

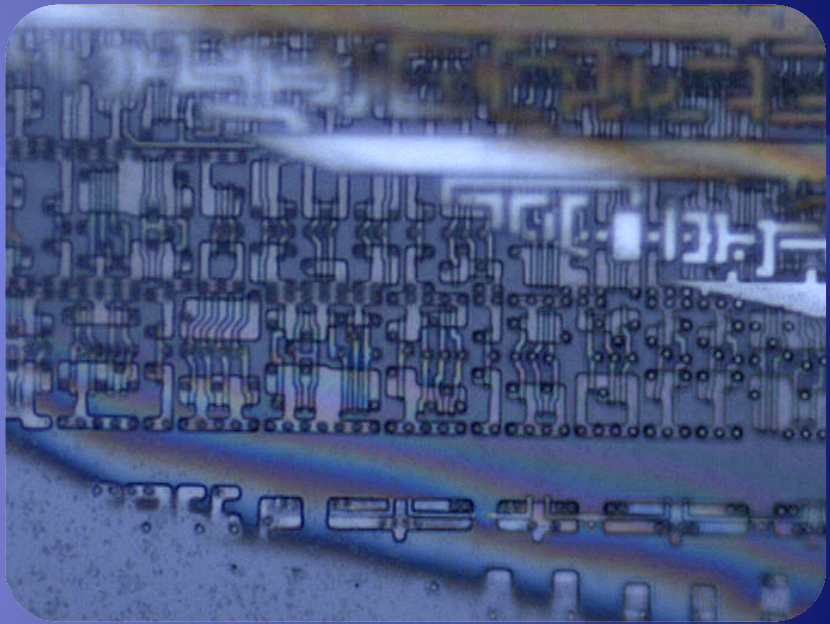
Mifare Classic RFID tag



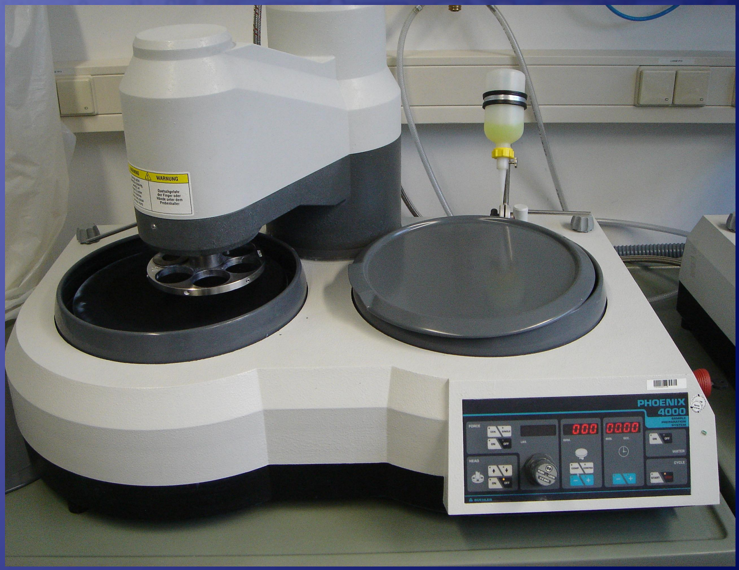


Polishing

- Embed chip in plastic
  - Downside: chip is tilted



- Automated polishing with machine
  –or–
  Manually with sand paper



- “On your kitchen table”

  -Starbug

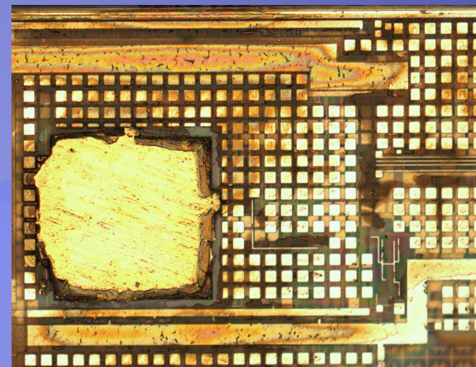
Imaging Chip

- Simple optical microscope
  - 500x magnification
  - Camera 1 Mpixel
  - Costs < $1000, found in most labs

- Stitching images
  - Panorama software (`hugin`)
  - Each image ~100x100 µm

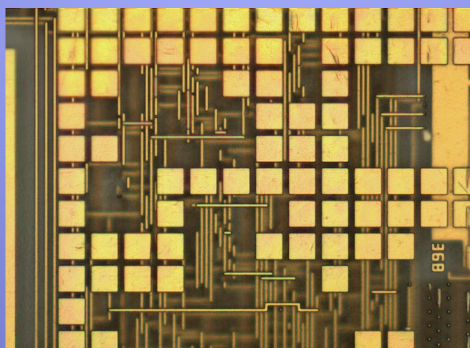
- Align different layers

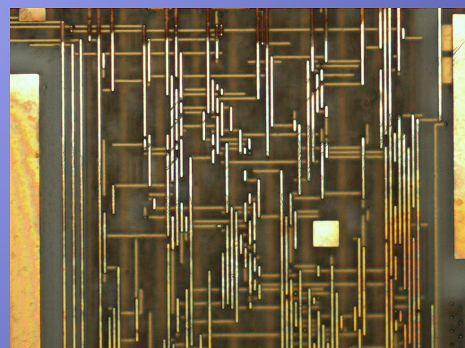
Chip Layers

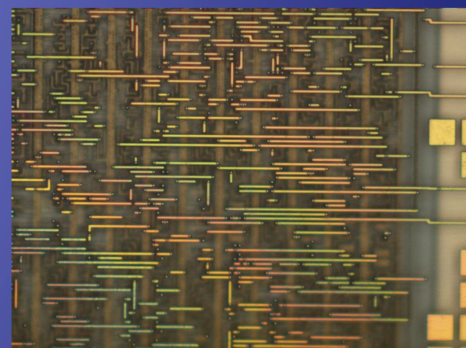


Cover layer

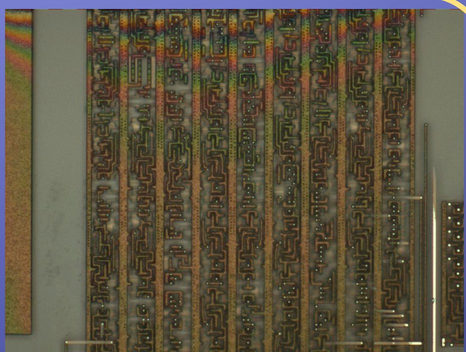
3 Interconnection layer

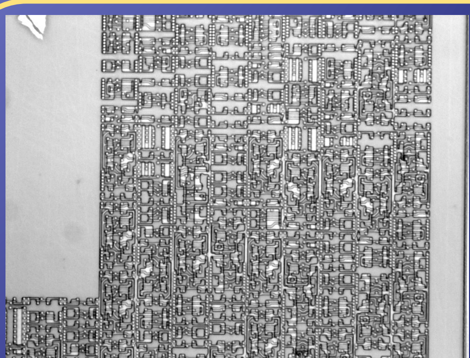






Logic layer

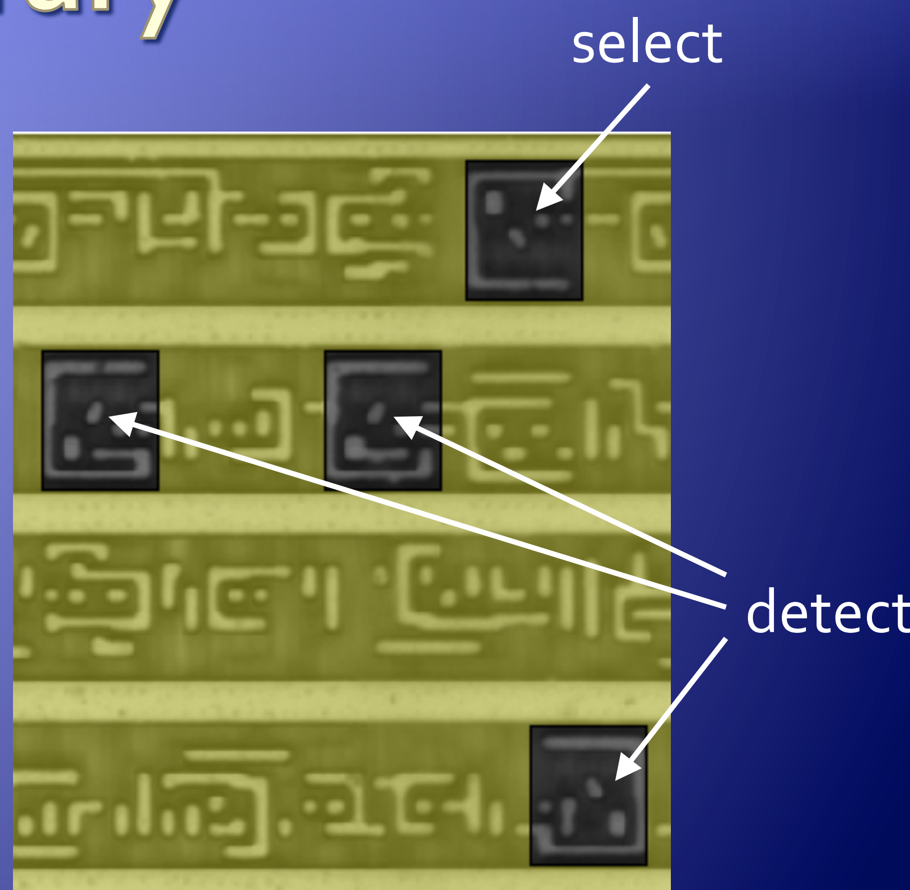




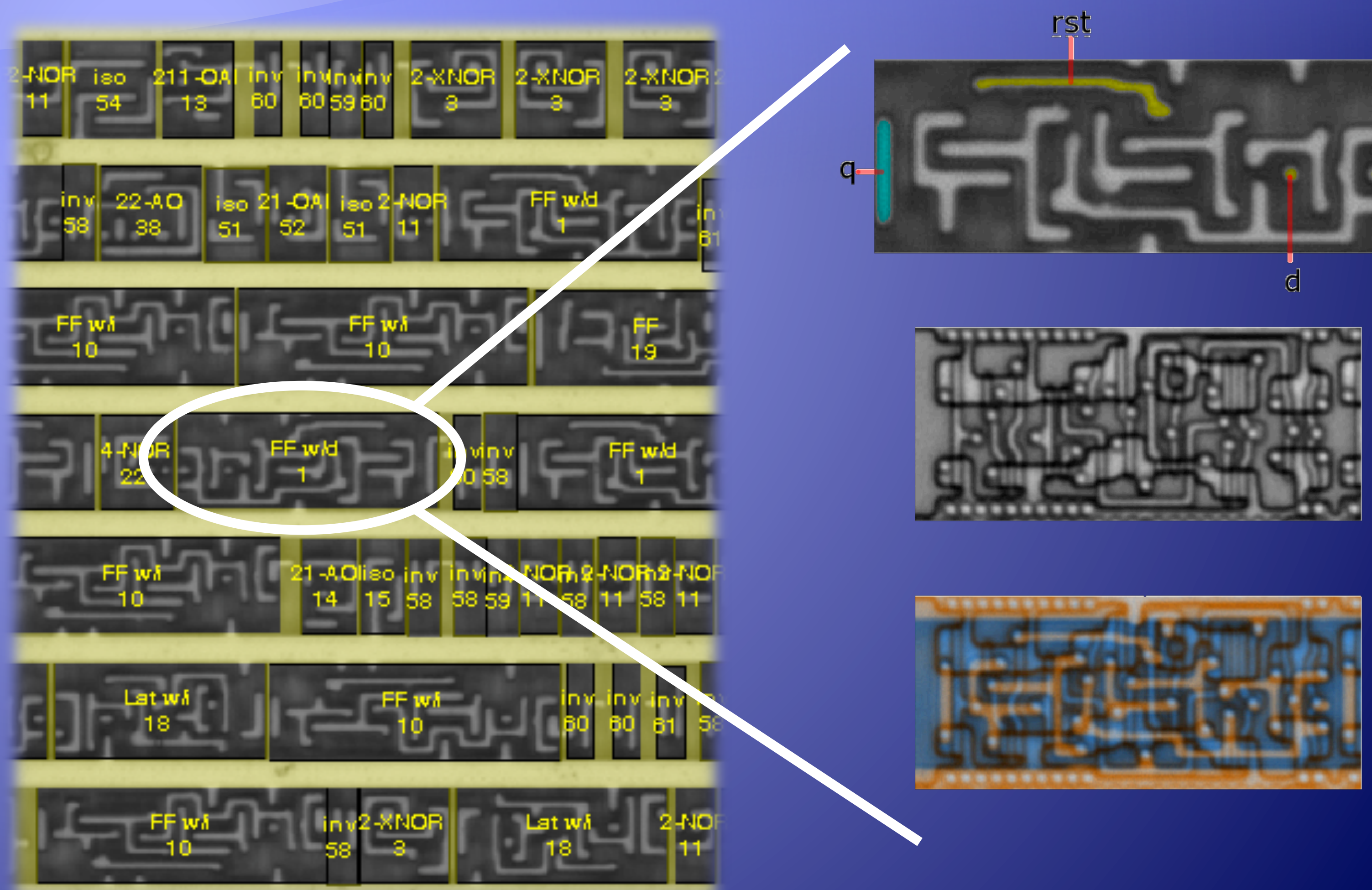
Transistor layer

Logic Gates Library

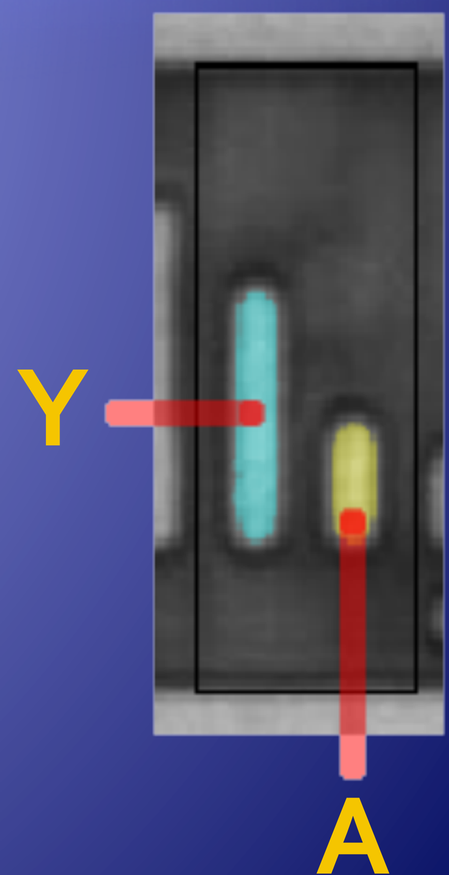
- Chip has several thousand gates on logic layer
- But only ~70 different types
  - Detection can be automated through template matching



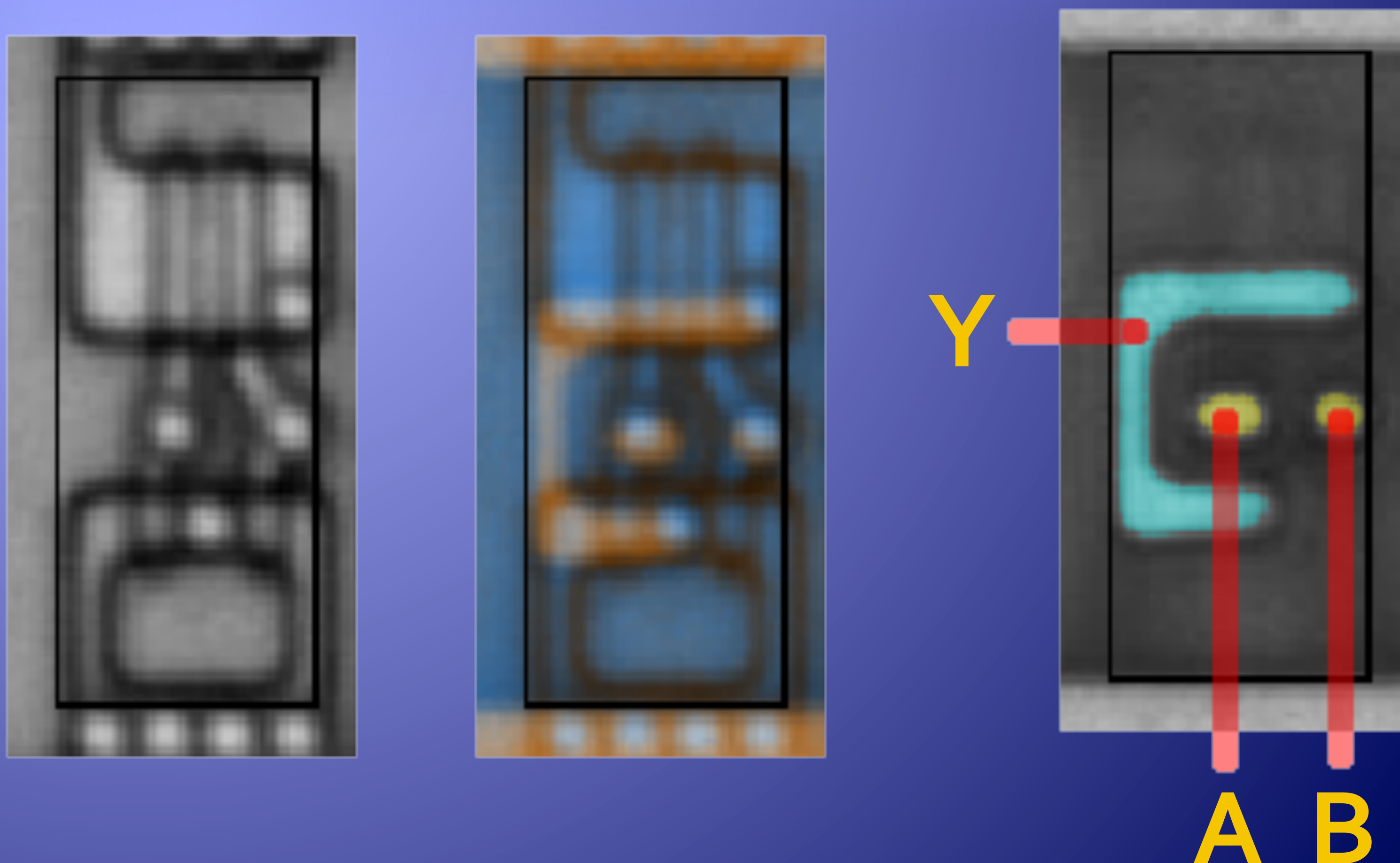
Logic Gates



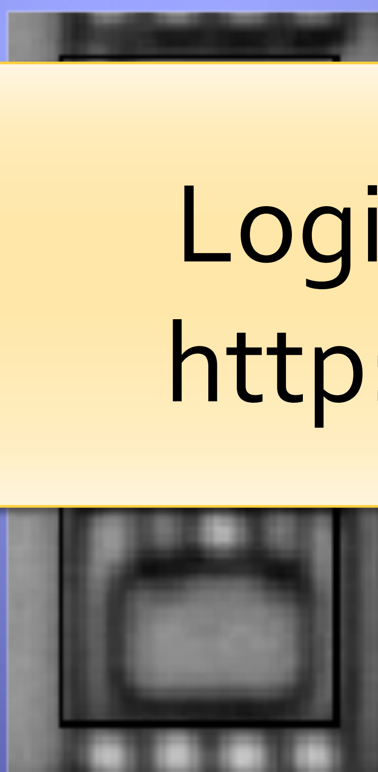
Logic Gates – Inverter

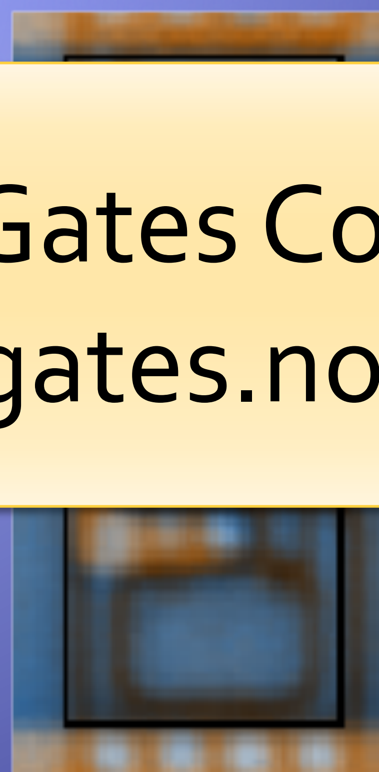


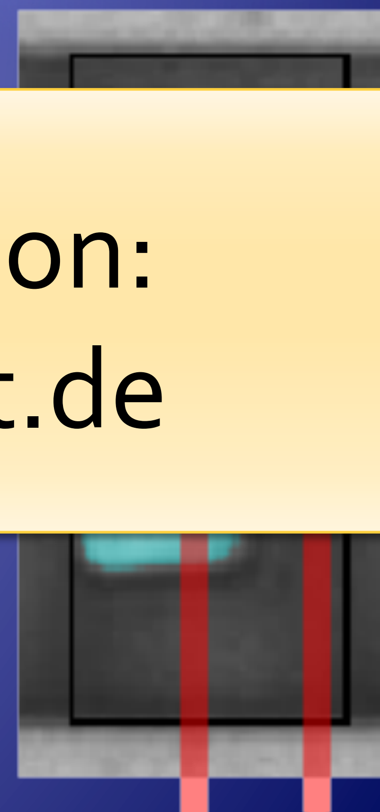
Logic Gates – 2NOR



Logic Gates – 2NOR







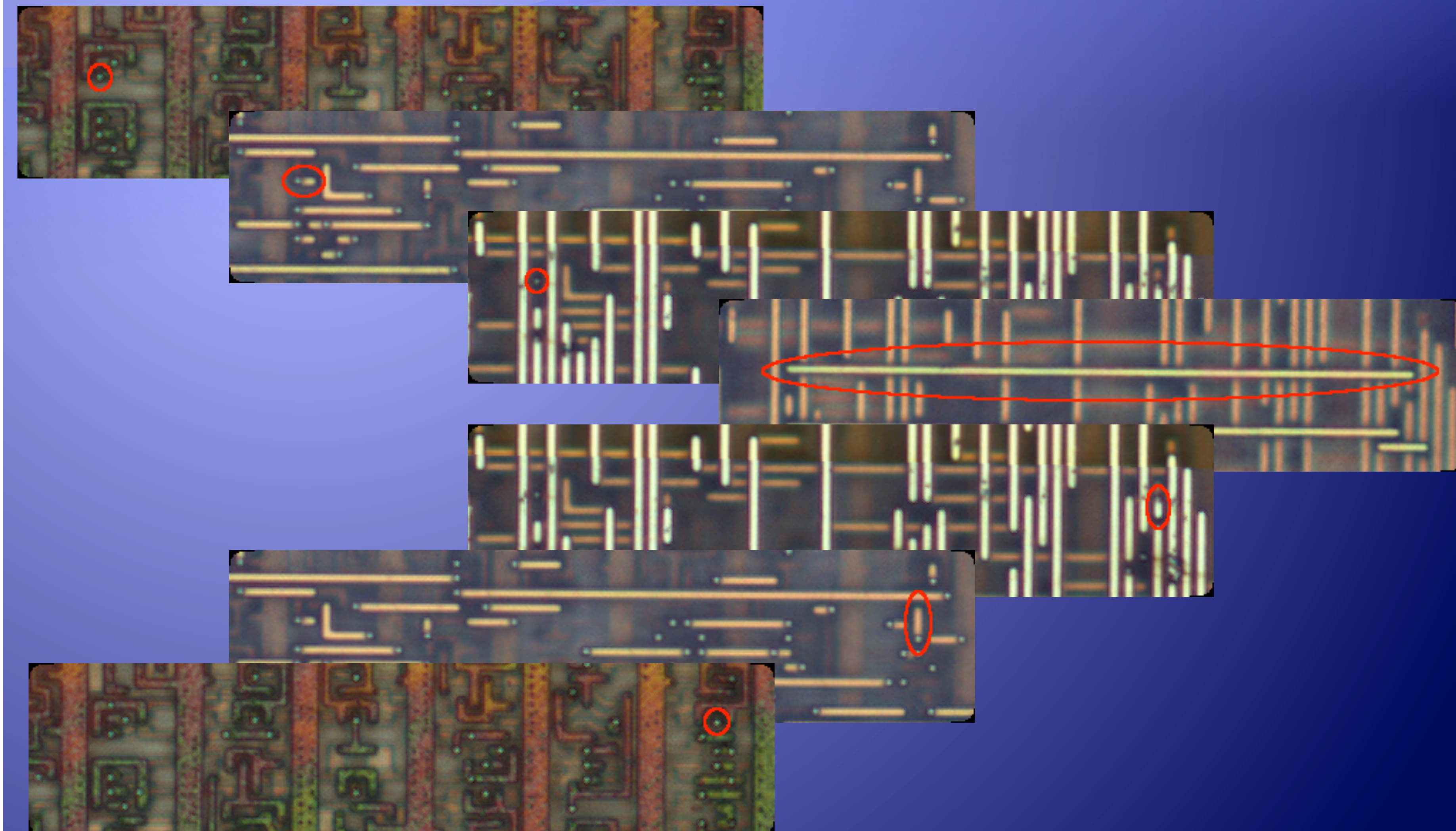
Logic Gates Collection:
http://gates.nohlnet.de

Logic Gates Interconnect

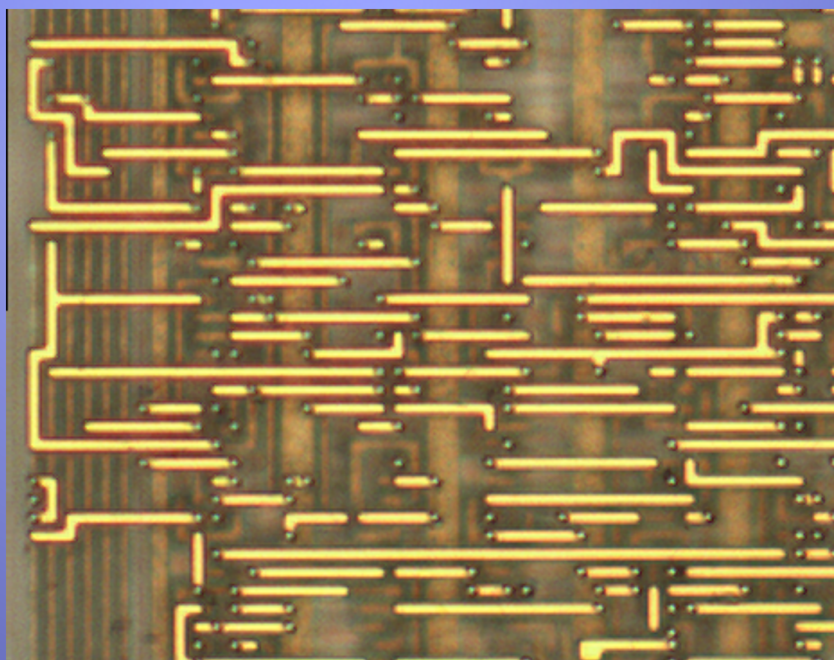
- Connections across all layers

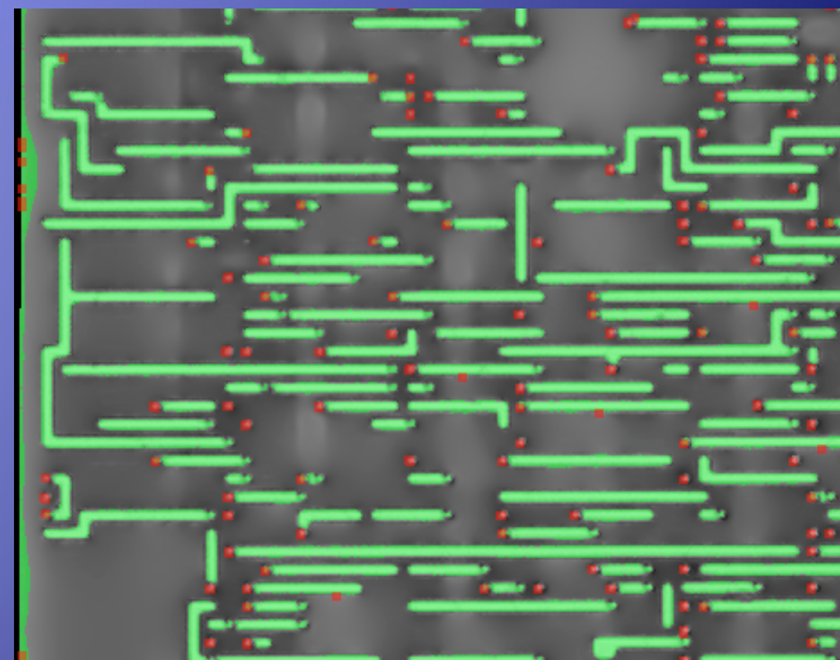
- Traced 1500 (!) connections manually
  - Tedious, time consuming
  - Error-prone (but errors easily spottable)
  - Tracing completely automated by now

Tracing Connections



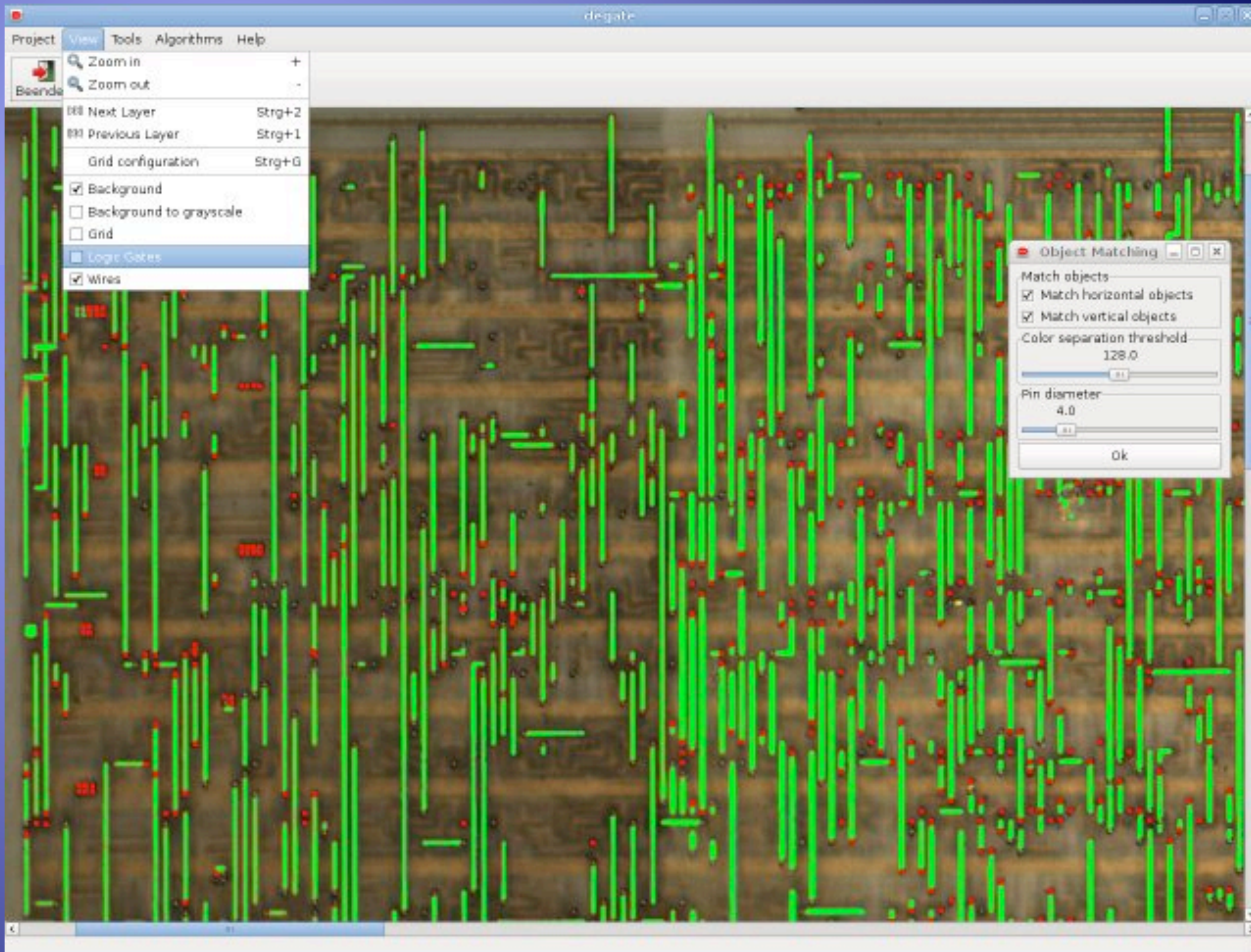
Automated Tracing



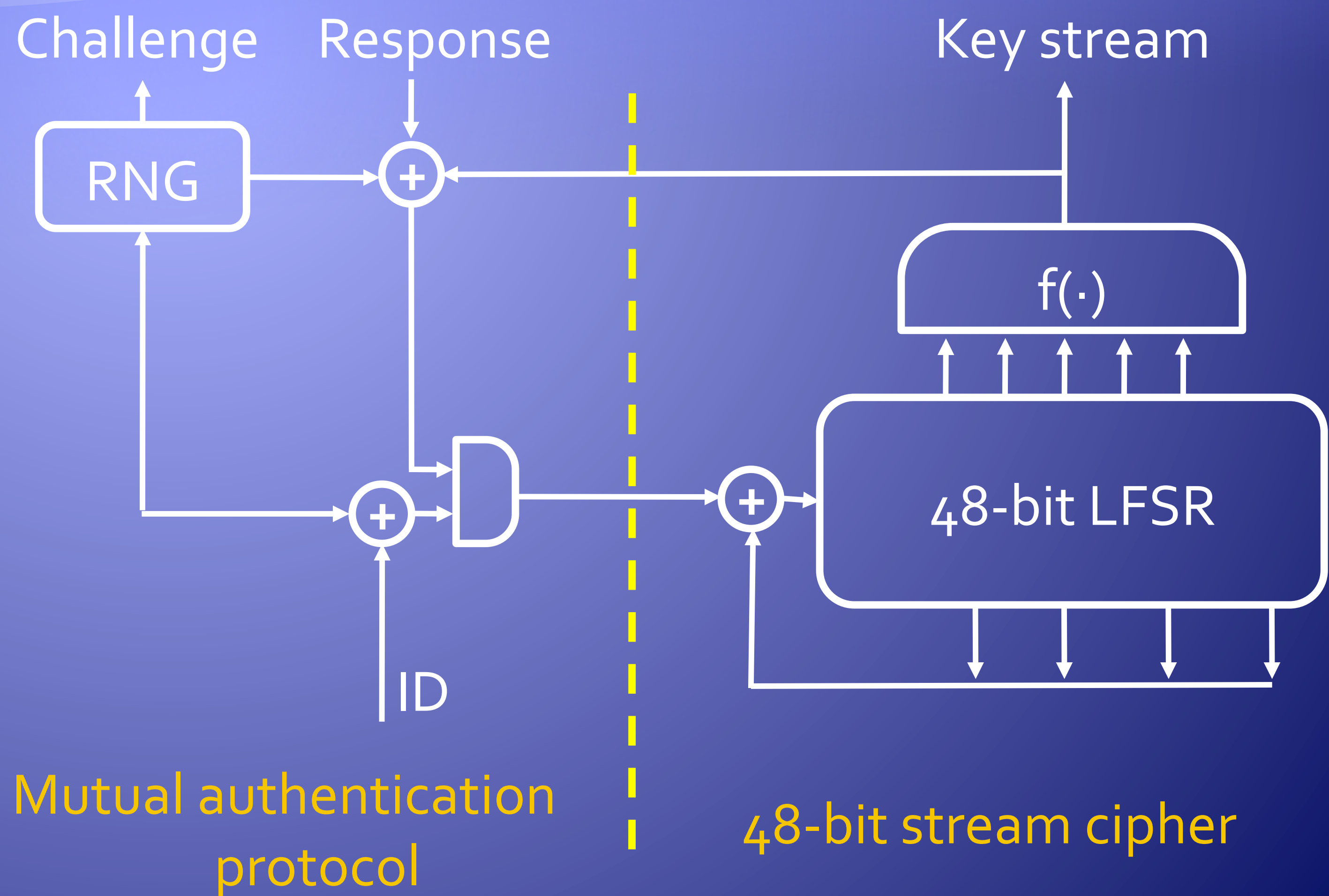


Metal wire

Intra-layer via

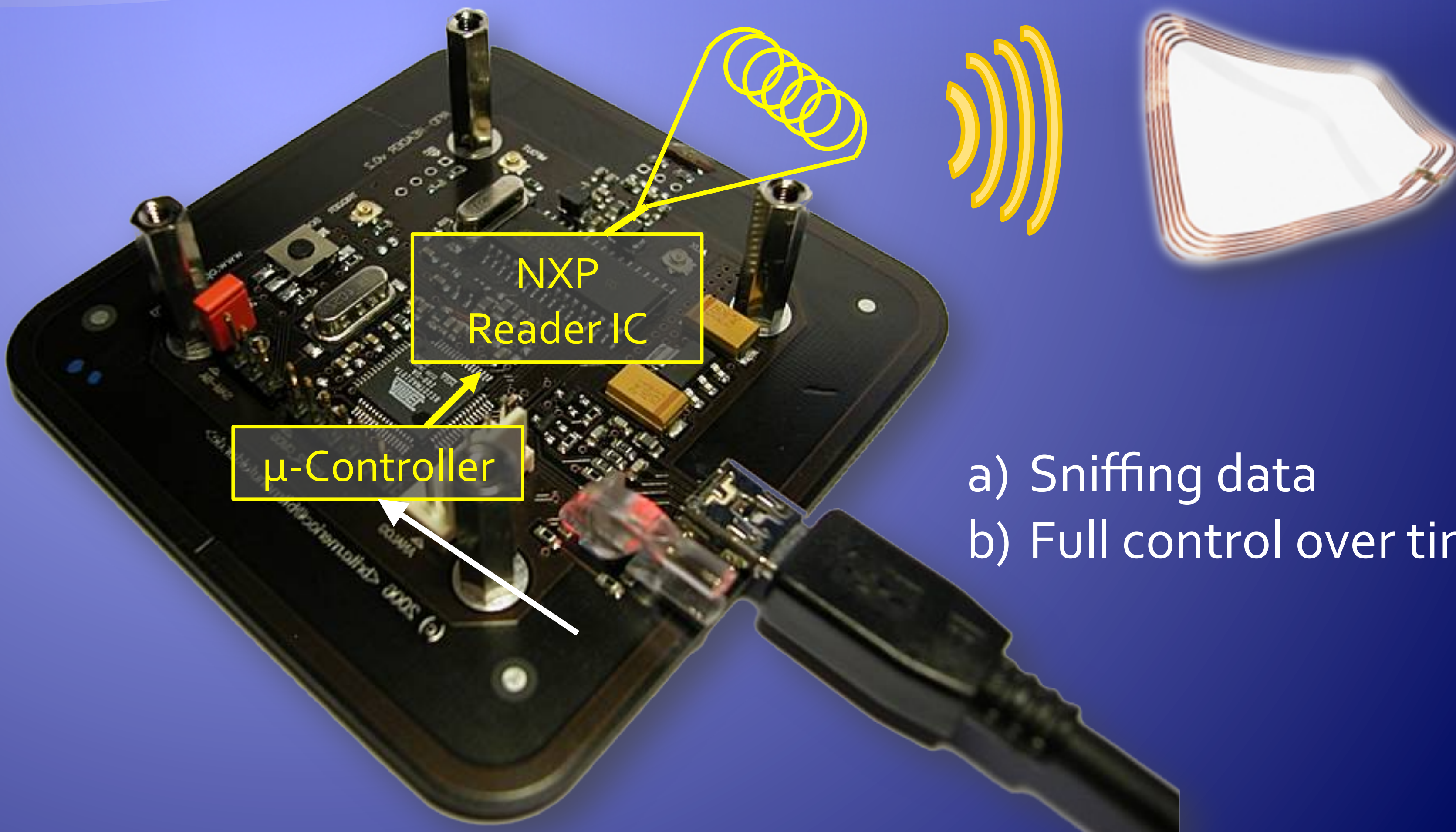

degate
Project
View
Tools
Algorithms
Help
Zoom in +
Zoom out -
Next Layer Strg+2
Previous Layer Strg+1
Grid configuration Strg+G
Background
Background to grayscale
Grid
Logic Gates
Wires
Object Matching
Match objects
Match horizontal objects
Match vertical objects
Color separation threshold
128.0
Pin diameter
4.0
Ok

Mifare Crypto-1



Vulnerabilities

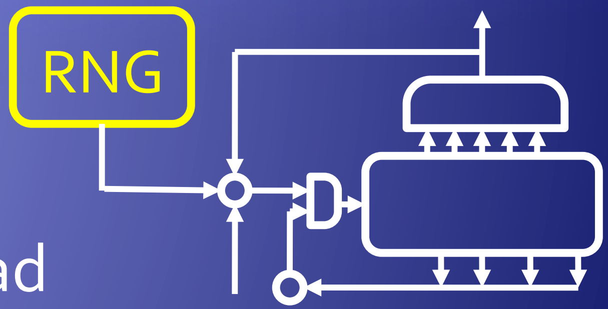
Hardware: OpenPCD (+PICC)



a) Sniffing data
b) Full control over timing!

Random Number Generator

- 16(!!)-bit random numbers
  - LFSR –based
  - Value determined by time of read



Our Attack:

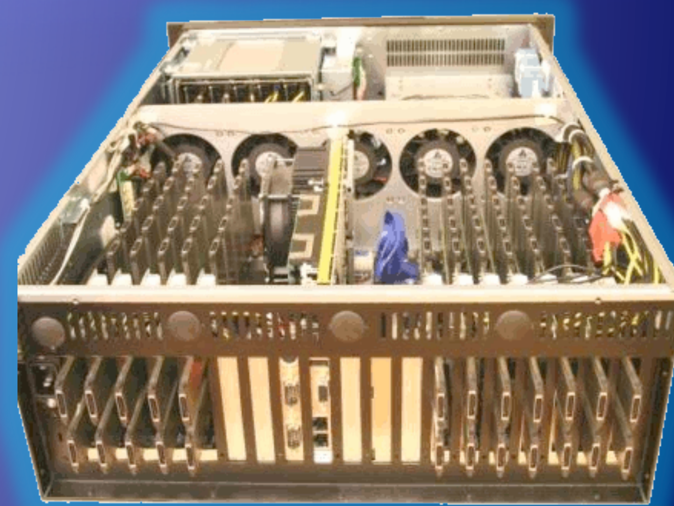
- Control timing (OpenPCD)

  = control random number (works for tag and reader!)

  = break Mifare security :)

For Starters: Brute-Force

- Cipher complexity low
  - Was probably a primary design goal
  - Very efficient FPGA implementation

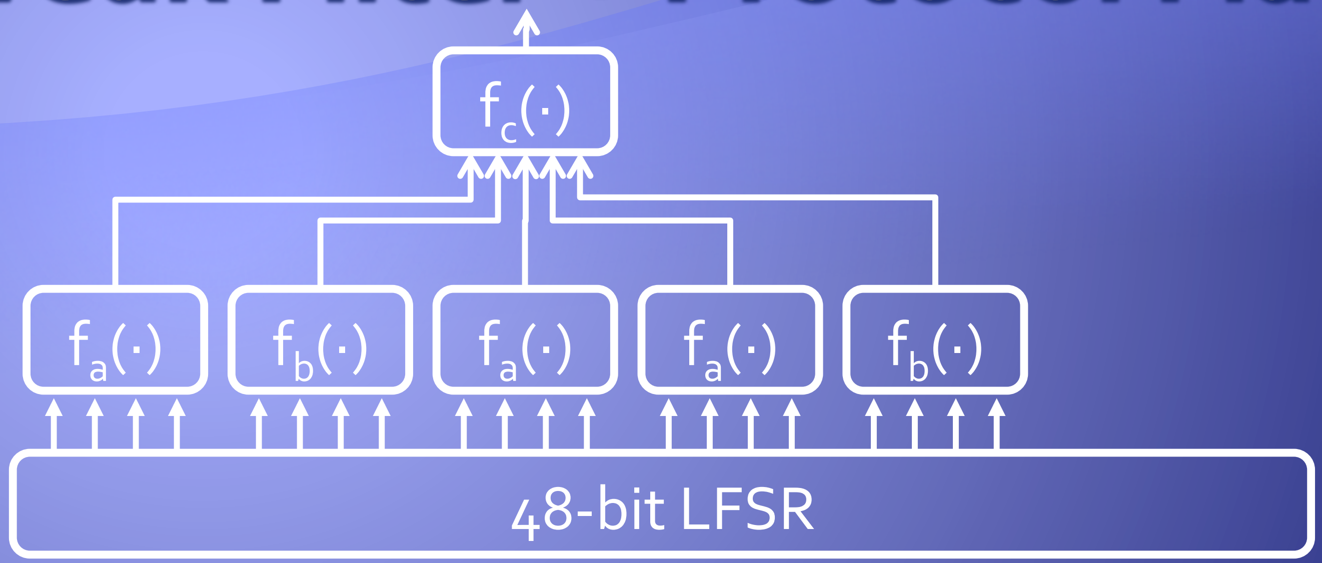


Source: Pico Comp.

FPGA cluster finds key
in 50 minutes!

30 sec. when trading space for time!!

Weak Filter + Protocol Flaw



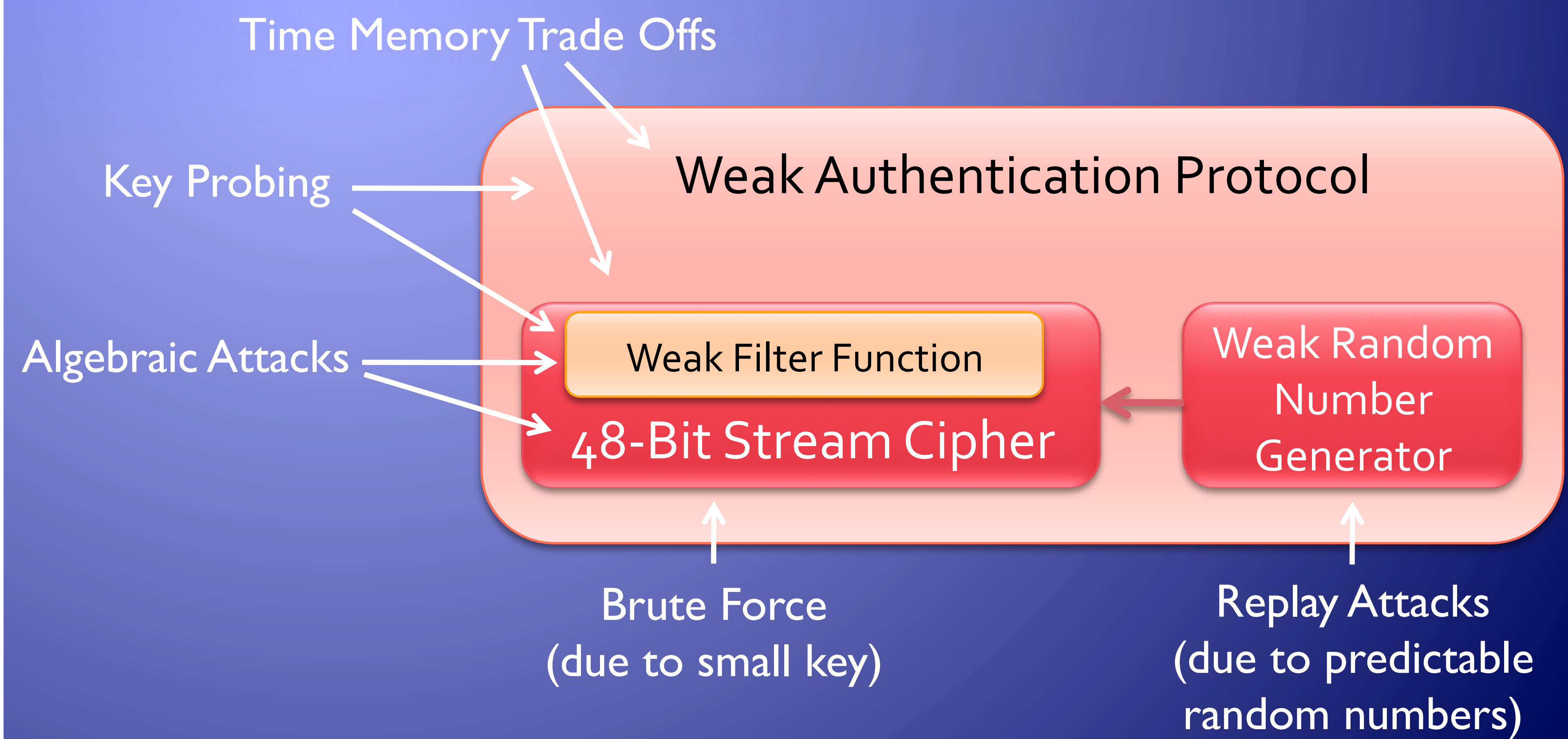
- Filter function is a network of smaller functions that are statistically biased
- Adversary controls inputs, can probe for internal state bits
- Attack takes < 1 minute on laptop

Algebraic Attacks

- Unpublished attacks that exploit simple feedback structure and statistical weaknesses
- Works for strong random numbers
  - Hence, even against Crypto-1 on Mifare Plus!

- Attack takes 30 seconds on laptop
- Stay tuned for publication …

Mifare Classic Weaknesses



Attack Properties

	Runtime on FPGA Cluster ($100,000)	Runtime on PC	Works despite strong random numbers (Mifare Plus)	Hard to Detect
Replay Attacks	(0)	(0)	No	No
Brute Force	50 min	—	**Yes**	**Yes**
Time Memory Trade Offs (TMTO)	30 sec	—	No	Maybe
Key Probing	—	1 min	No	No
Algebraic Attacks	—	**30 sec**	**Yes**	**Yes**

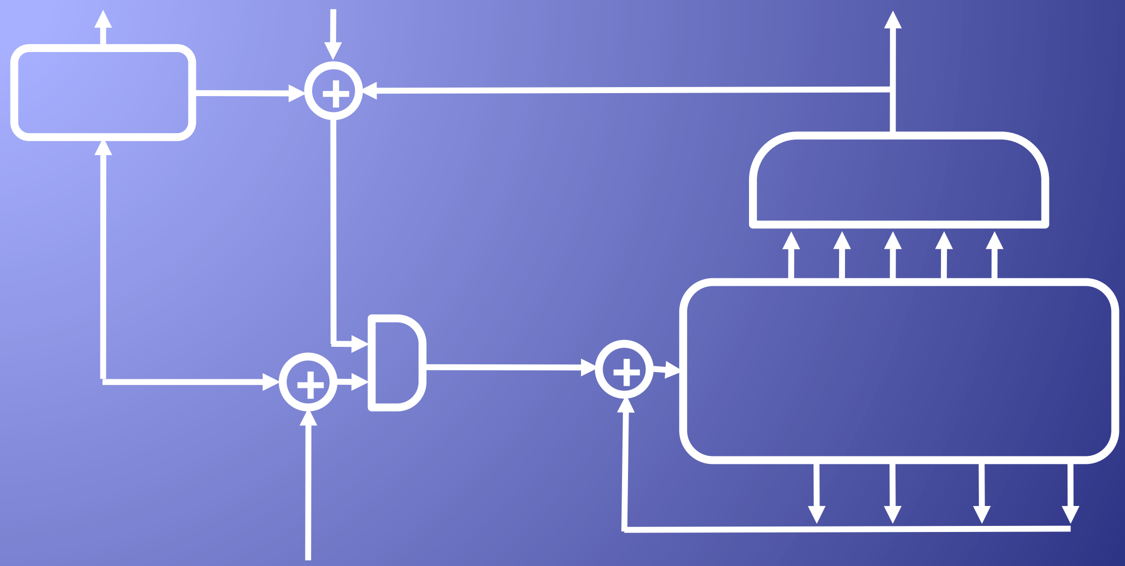
Mifare Security

- Protection insufficient for almost all uses:
  - Access control, car theft protection, credit cards, …
- Perhaps good enough for privacy

Lessons Learned

- Reverse-Engineering is possible
  - you should try! (I'll help)
- Obscurity add security only in the short-run
  - (but lack of peer-review hurts later)
- RFID constraints make good crypto very hard
  - How much security is needed?
  - How much more expensive is privacy?

Questions?



Karsten Nohl
nohl@virginia.edu

Talk to me about your reverse-engineering ideas!