CCC '07

Karsten Nohl, Starbug, Henryk Plötz

MIFARE SECURITY

RFID tags

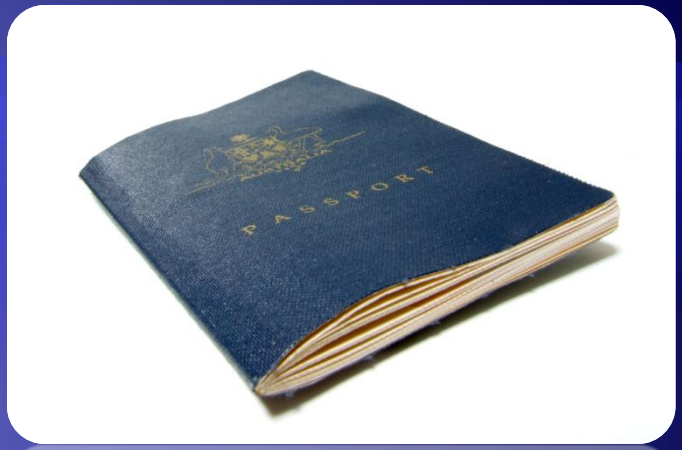
- Radio Frequency IDentification
- Tiny computer chips
- Passively Powered

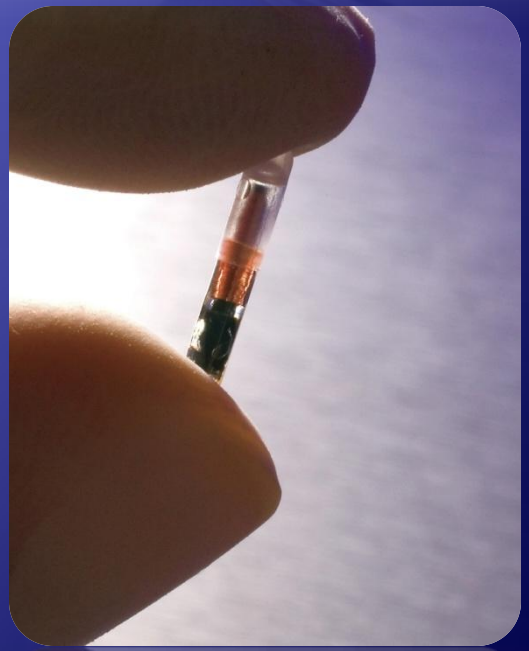
RFID Applications

- RFIDs become ubiquitous
- Integrated in many *security* applications
  - Tickets
  - Access Control
  - Car Ignition

RFID Trends

- Passports
- Implants
- …





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

RFID Trends (II)

- Tagging of consumer goods
  - Will replace bar-codes!
- Threat to *Privacy*
  - Customer tracking
  - Leaks internal business information!

RFID Tre

- Tagging of c
  - Will replace
- Threat to *Pr*
  - Customer t
  - Leaks inter

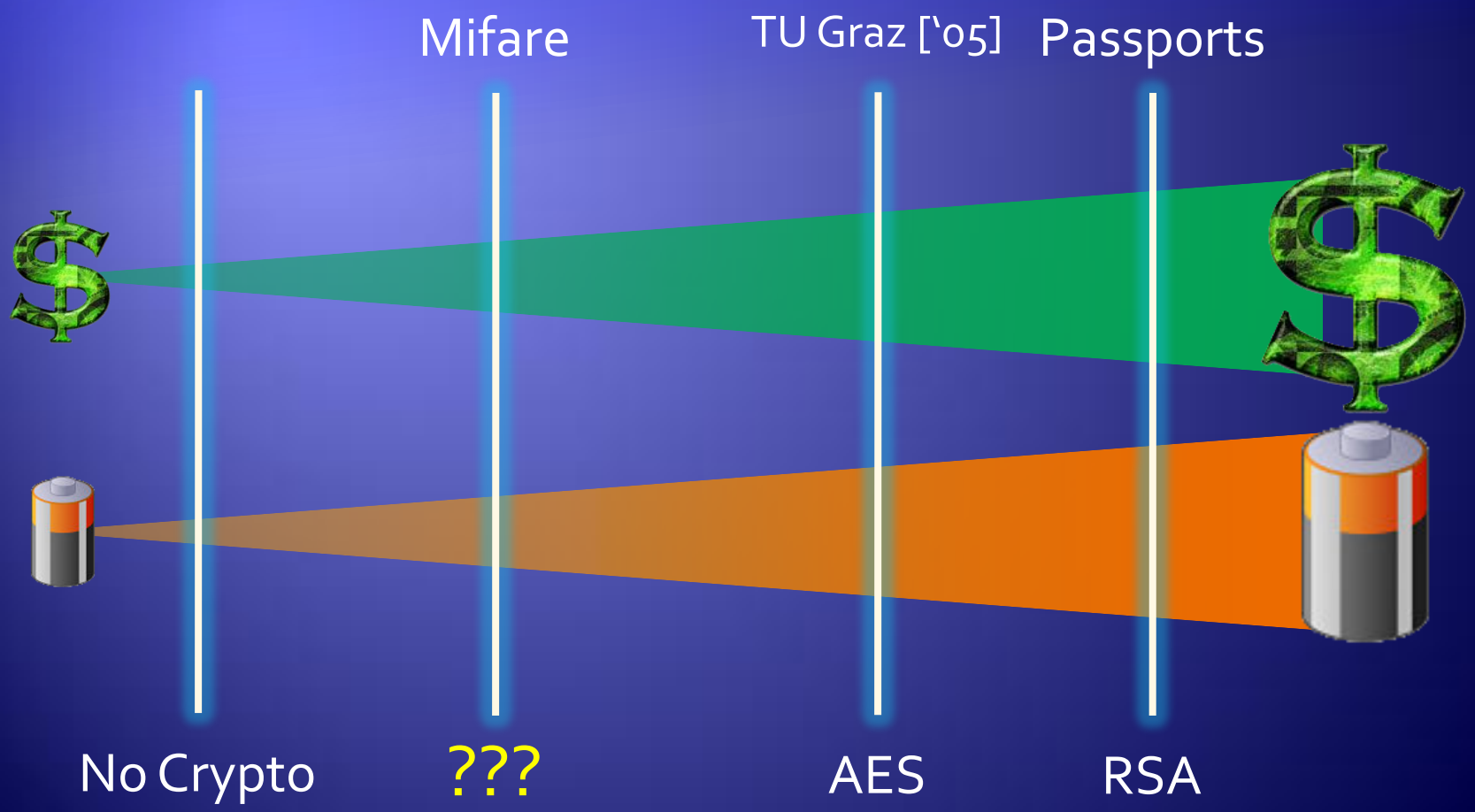
Motivation

Cryptography on RFIDs in needed for:

- Unclonability
  - Credit cards, luxury goods, medication, …
- Privacy!

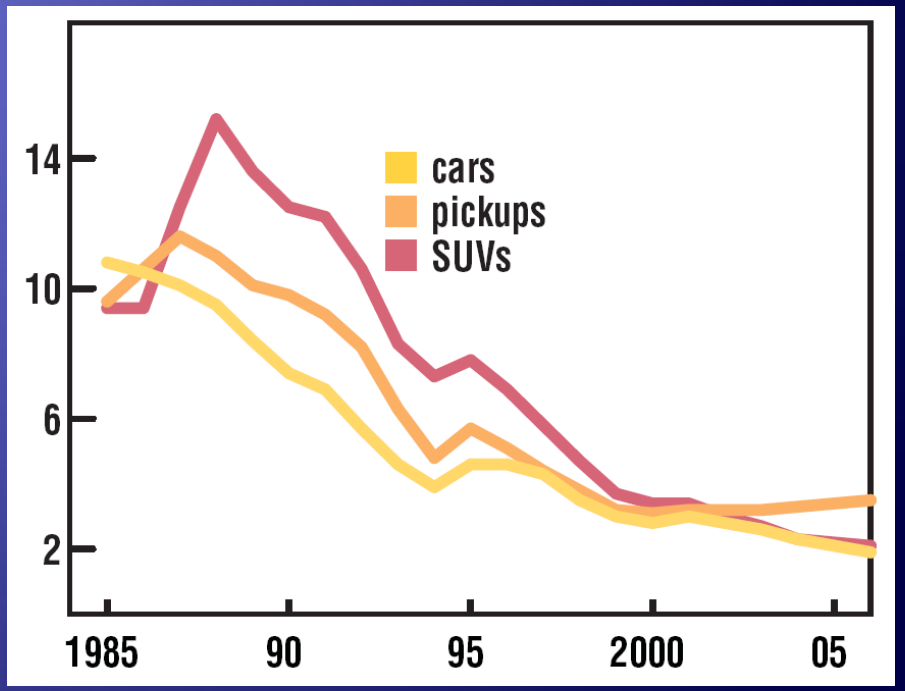
But, what crypto is small enough for tags?

RFID-Crypto Mismatch



Mifare Security

- Philips claims:
  - "approved authentication"
  - "advanced security levels"
- 48 bit key



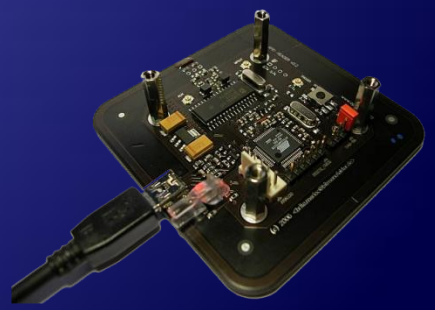
Car thefts
(source: hldi.org)

Our Project

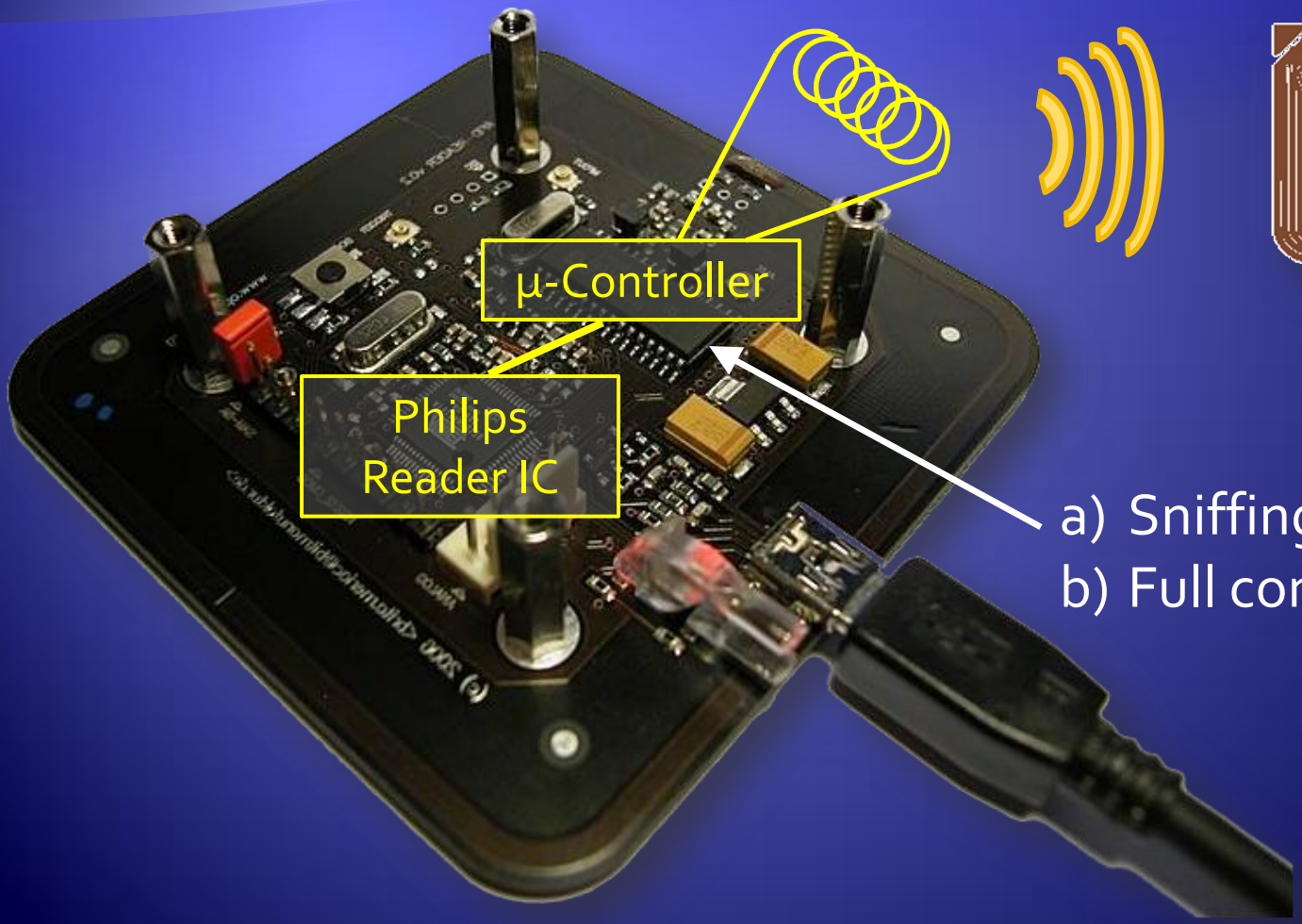
Reverse-engineering of the Mifare crypto and evaluating its security

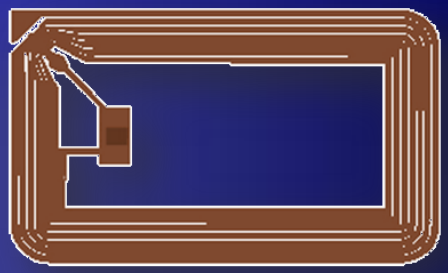
- Reconstruct circuit from photos of chip
- Sniff reader-tag communication

verify



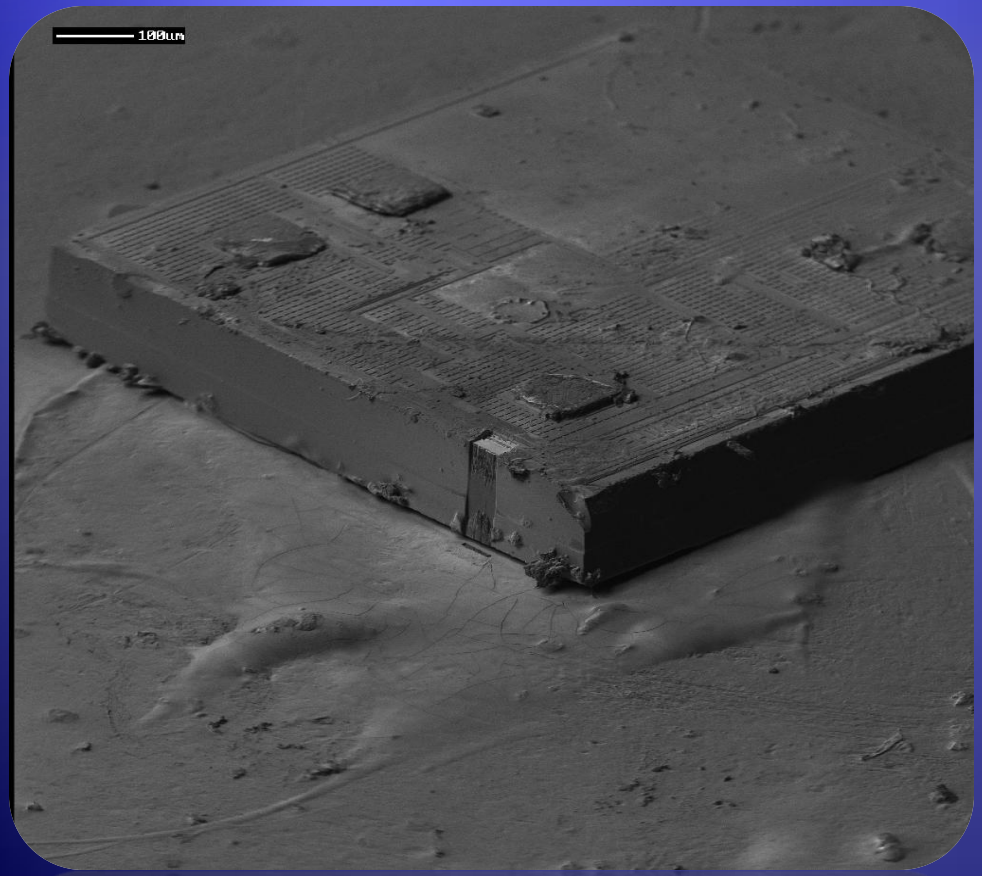
Hardware: OpenPCD (+PICC)



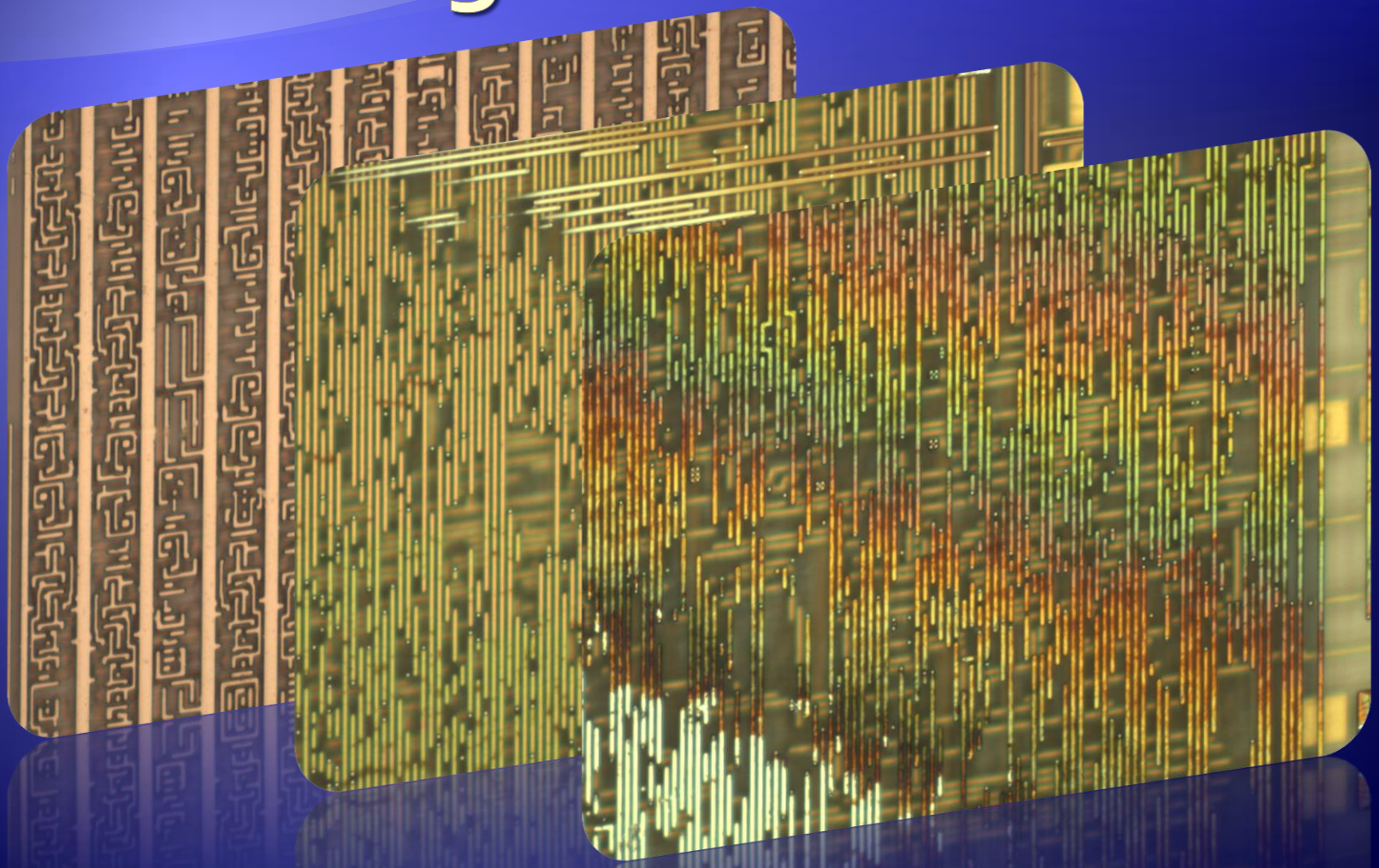


a) Sniffing data
b) Full control over timing!

Mifare RFID tag

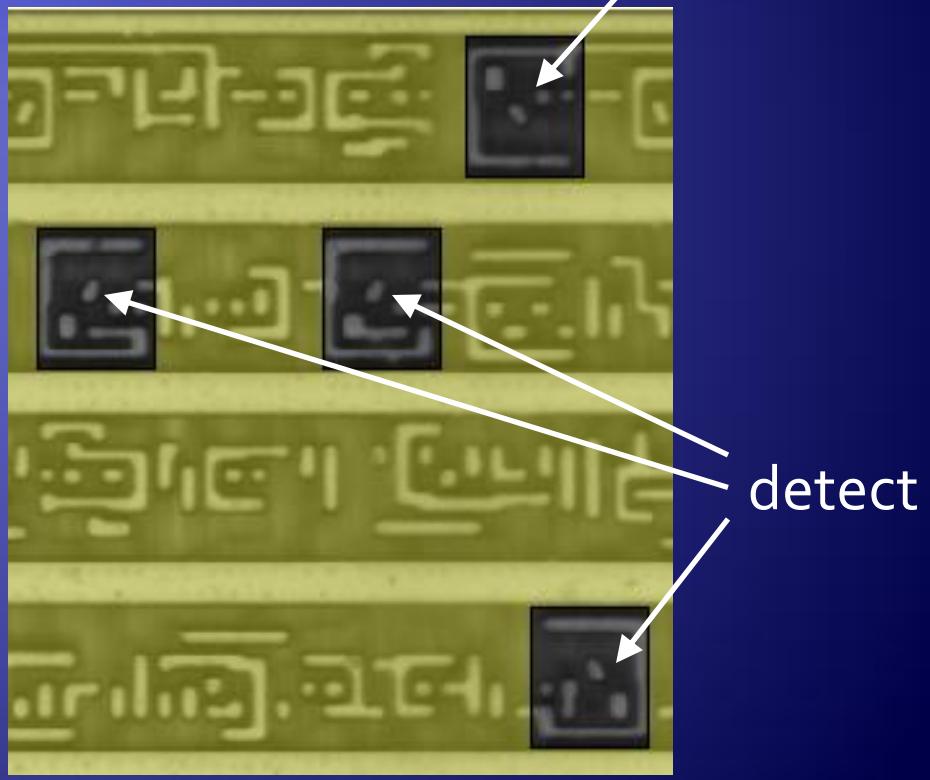


Circuit Images



Step 1: build library

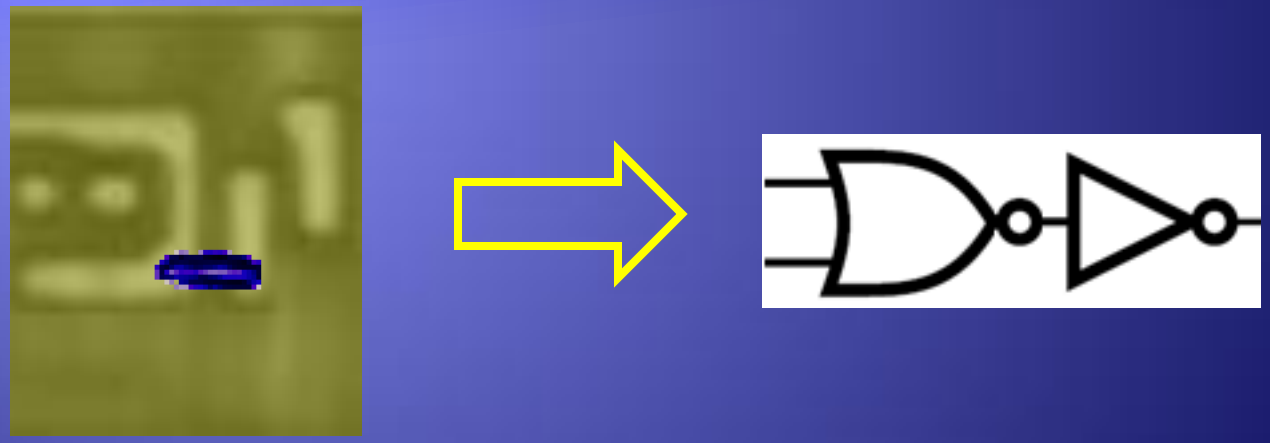
- Chip has several thousand gates
- But only ~70 different types
  - Detection can be automated



Step 2: Encircle Crypto

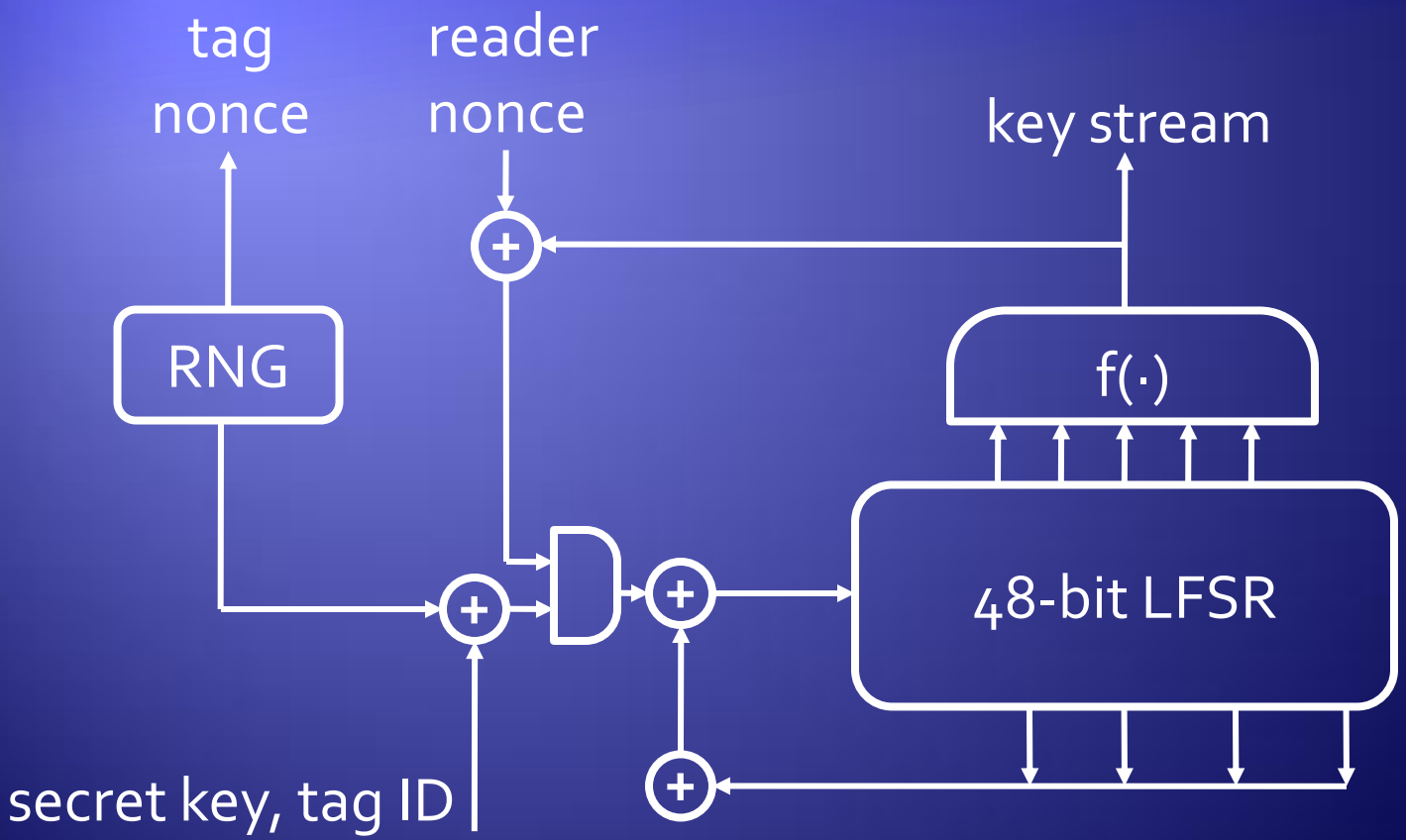
- Even tiny RFID chip too large to analyze entirely
  - Crypto <10% of gates!
- Focus on interesting-looking parts:
  - Strings of flip-flops (registers)
  - XOR
  - Units around edges that sparsely connected to the rest of the chip

Step 3: Reproduce Circuit



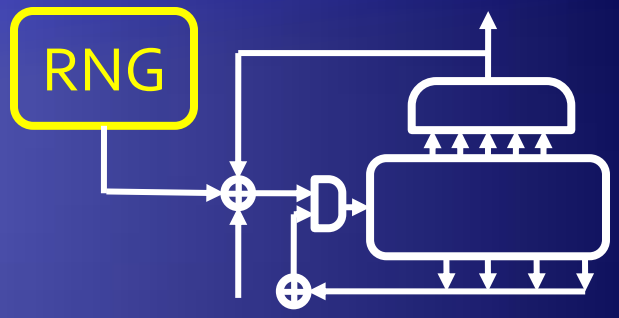
- Very error-prone and tedious process
  - Will automate further

Mifare Crypto-1



Random Number Generator

- 16(!!)-bit random numbers
  - LFSR –based
  - Value derived from time of read



Our Attack:

- Control timing (OpenPCD)

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

  = break Mifare security :)

Linear feedback shift register

From Wikipedia, the free encyclopedia
(Redirected from LFSR)

A **linear feedback shift register** (LFSR) is a shift register whose input bit is a linear function of its previous

The only linear functions of single bits are xor and inverse-xor; thus it is a shift register whose input bit is driv

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeat which appears random and which has a very long cycle.

Applications of LFSRs include generating pseudo-random numbers, pseudo-noise sequences, fast digital cou common.

Fibonacci LFSRs

The list of the bits' positions that affect the next state is called the tap sequence. In the diagram below, the s the output and then feed back into the leftmost bit.

- The outputs that influence the input are called *taps* (blue in the diagram below).
- A maximal LFSR produces an n-sequence (i.e. cycles through all possible $2^n - 1$ states within the shift reg never change.

The sequence of numbers generated by an LFSR can be considered a binary numeral system just as valid as

The tap sequence of an LFSR can be represented as a polynomial mod 2. This means that the coefficients of polynomial. For example, if the taps are at the 16th, 14th, 13th and 11th bits (as below), the resulting LFSR p

$$x^{16} + x^{14} + x^{13} + x^{11} + 1$$

The 'one' in the polynomial does not correspond to a tap - it corresponds to the input to the first bit (i.e. x^0, wh
The first and last bits are always connected as an input and tap respectively.

WIKIPEDIA
The Free Encyclopedia

navigation
- Main Page
- Contents
- Featured content
- Current events
- Random article

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

search
Go Search

toolbox
- What links here
- Related changes
- Upload file
- Special pages

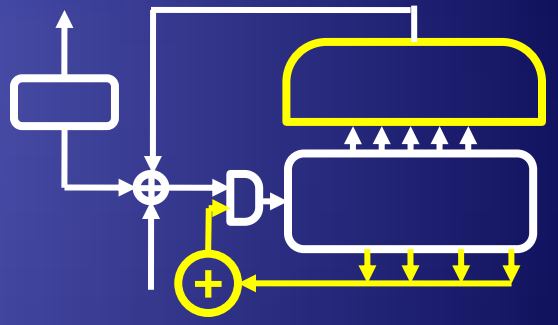
Structural Weaknesses

1) No non-linear component in feedback loop

→ No forward secrecy

2) Output bit derived from fixed subset of bits

→ non-optimal avalanche properties



Suggests attack on key faster than brute-force (known-plaintext)

Brute-Force Attack

- Cipher complexity low
  - Has probably been the highest design goal
  - Allows for very efficient FPGA implementation

$100 key cracker will find key in ~1 week! (much faster even when trading space for time)

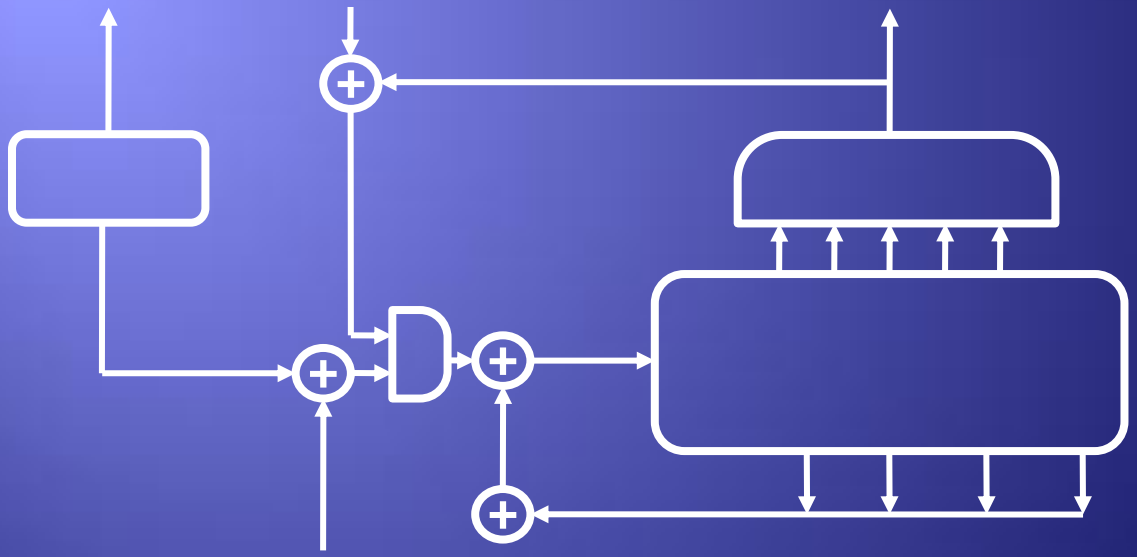
Mifare Security

- Protection perhaps sufficient to protect transactions of very small value
  - E.g., Micro-payments, privacy
- Security too weak for:
  - Access control, car theft protection, credit cards, …

Lessons Learned

- Obscurity and proprietary crypto add security only in the short-run
  - (but lack of peer-review hurts later)
- Constraints of RFIDs make good crypto extremely hard
  - Where are the best trade-offs?
  - How much security is needed?

Questions?



Karsten Nohl
nohl@virginia.edu