Analyzing RFID Security

Karsten Nohl
University of Virginia

Henryk Plötz
HU Berlin

Target: RFID tags

- **R**adio **F**requency **ID**entification
- Tiny computer chips
- Passively Powered

Ubiquitous Identification

- Constant monitoring is already part of our lives

- Trend is amplified through pervasive electronics, RFIDs

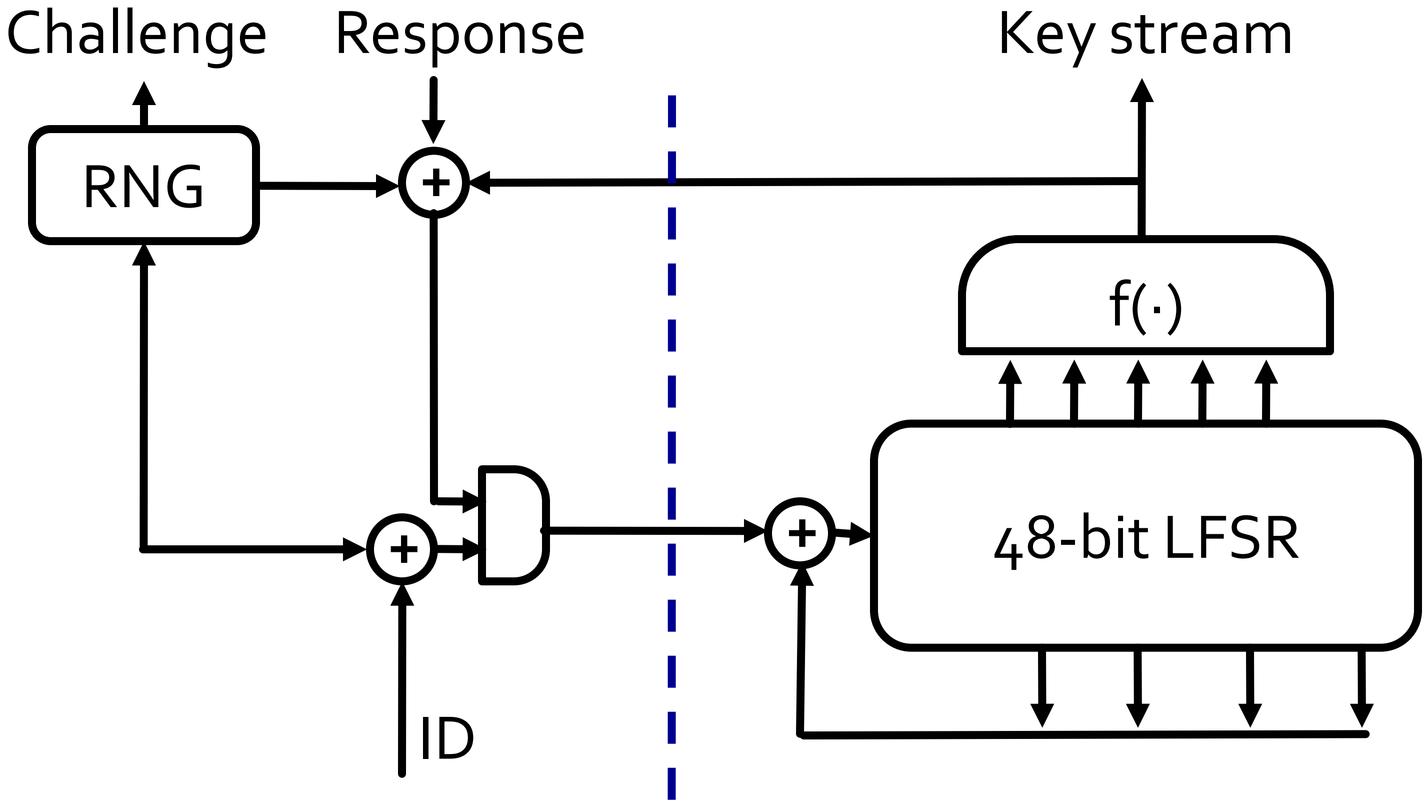
- Businesses will soon be able to track individuals

Privacy Impact of RFIDs

- RFID tags become universal identifier
  - For people: passports, credit cards, …
  - For products: bar code replacement
- Billions of RFIDs in circulations
  - Product tagging not started yet
- Privacy has so far been neglected
  - Destroying tags only realized privacy mechanism
  - More elegant solutions considered too expensive

Security building blocks on RFID tags are insufficient
for privacy applications.

Mifare Crypto-1



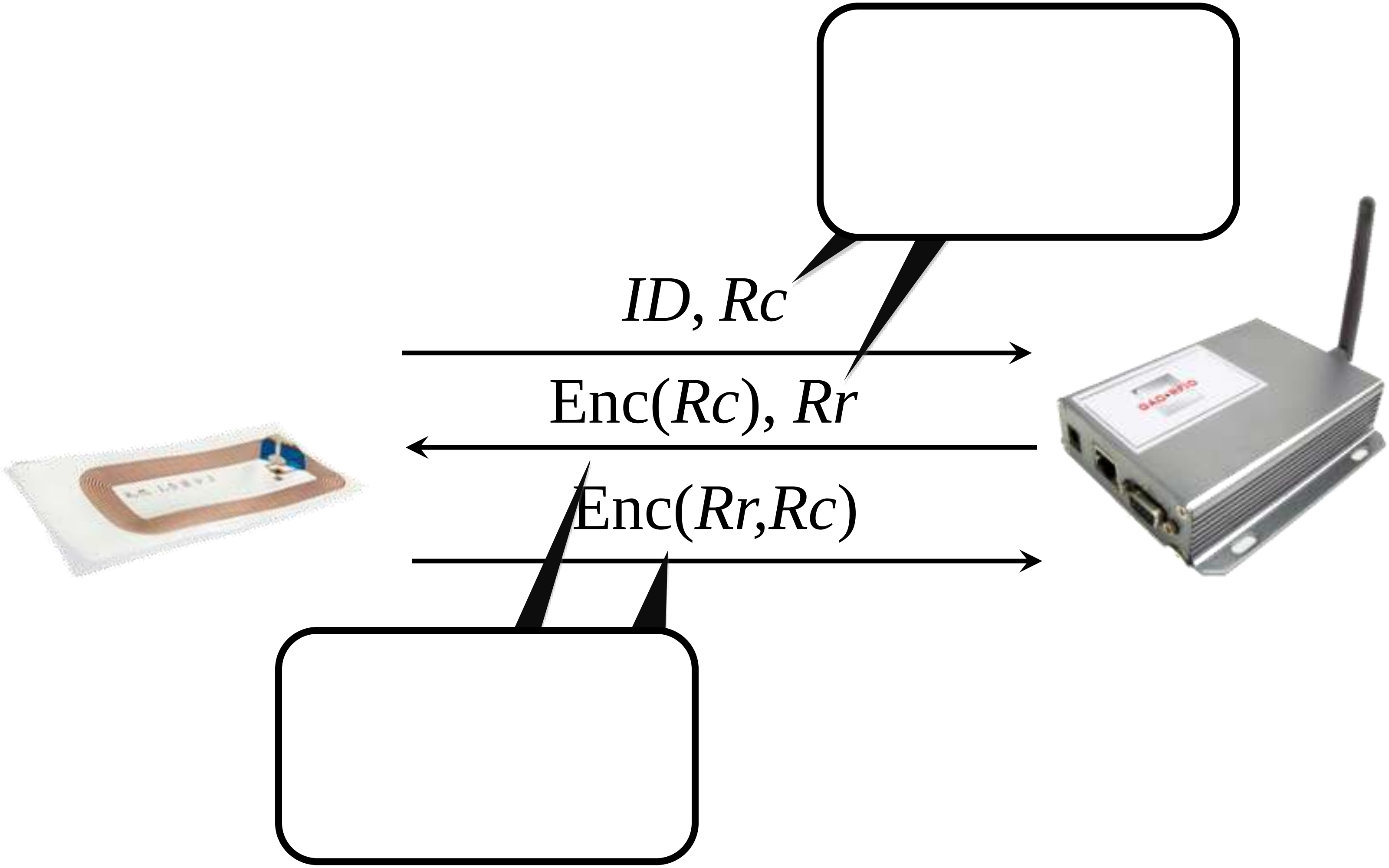
Mutual authentication protocol

48-bit stream cipher

Outline

- Attacks
  - From general to Mifare
- Countermeasures
  - And why they often fail
- Tools
  - We release today:
    - Sniffer, Fuzzer, Emulator

Challenge-Response Authentication

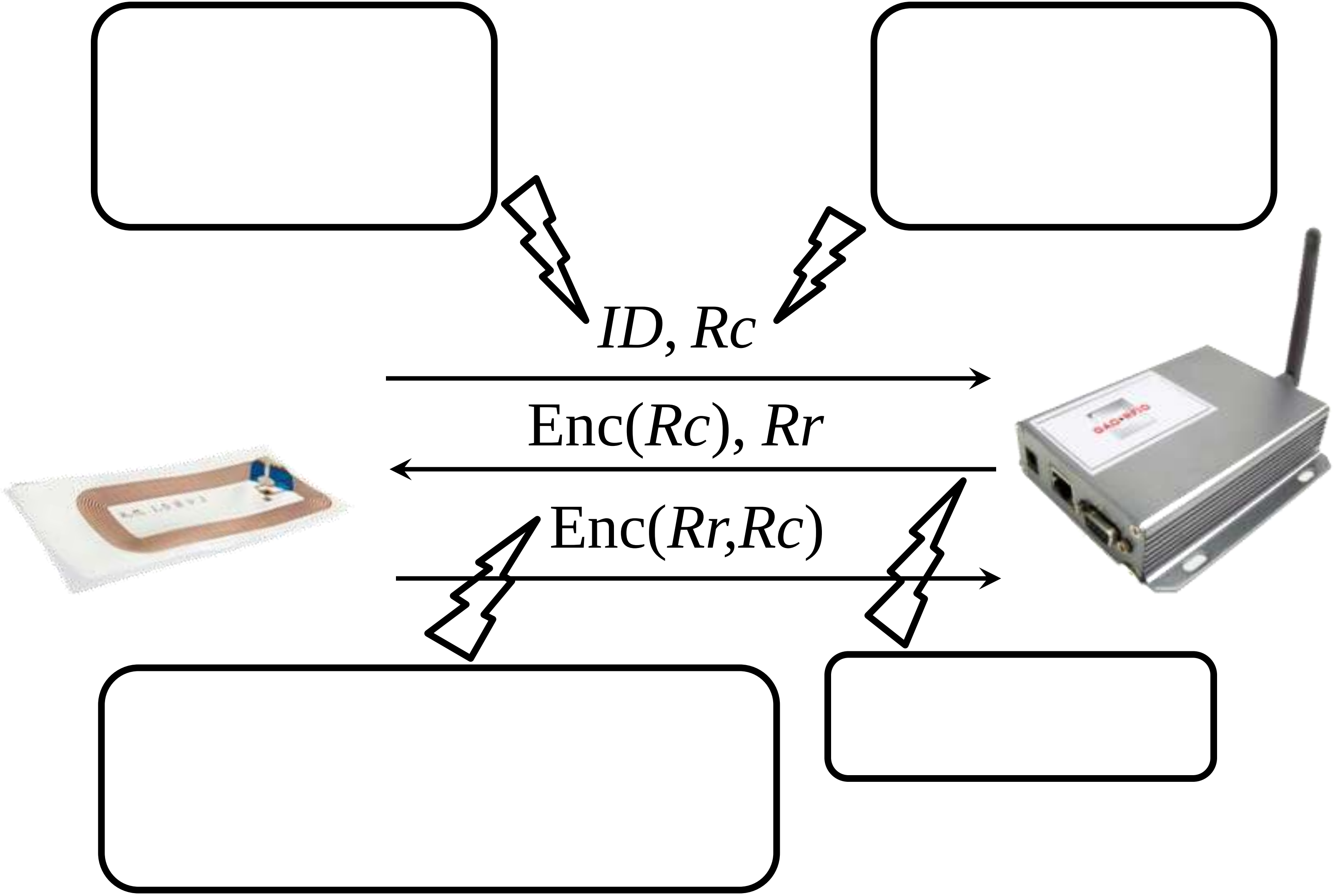


ID, *Rc*

Enc(*Rc*), *Rr*

Enc(*Rr*,*Rc*)

Attack Space

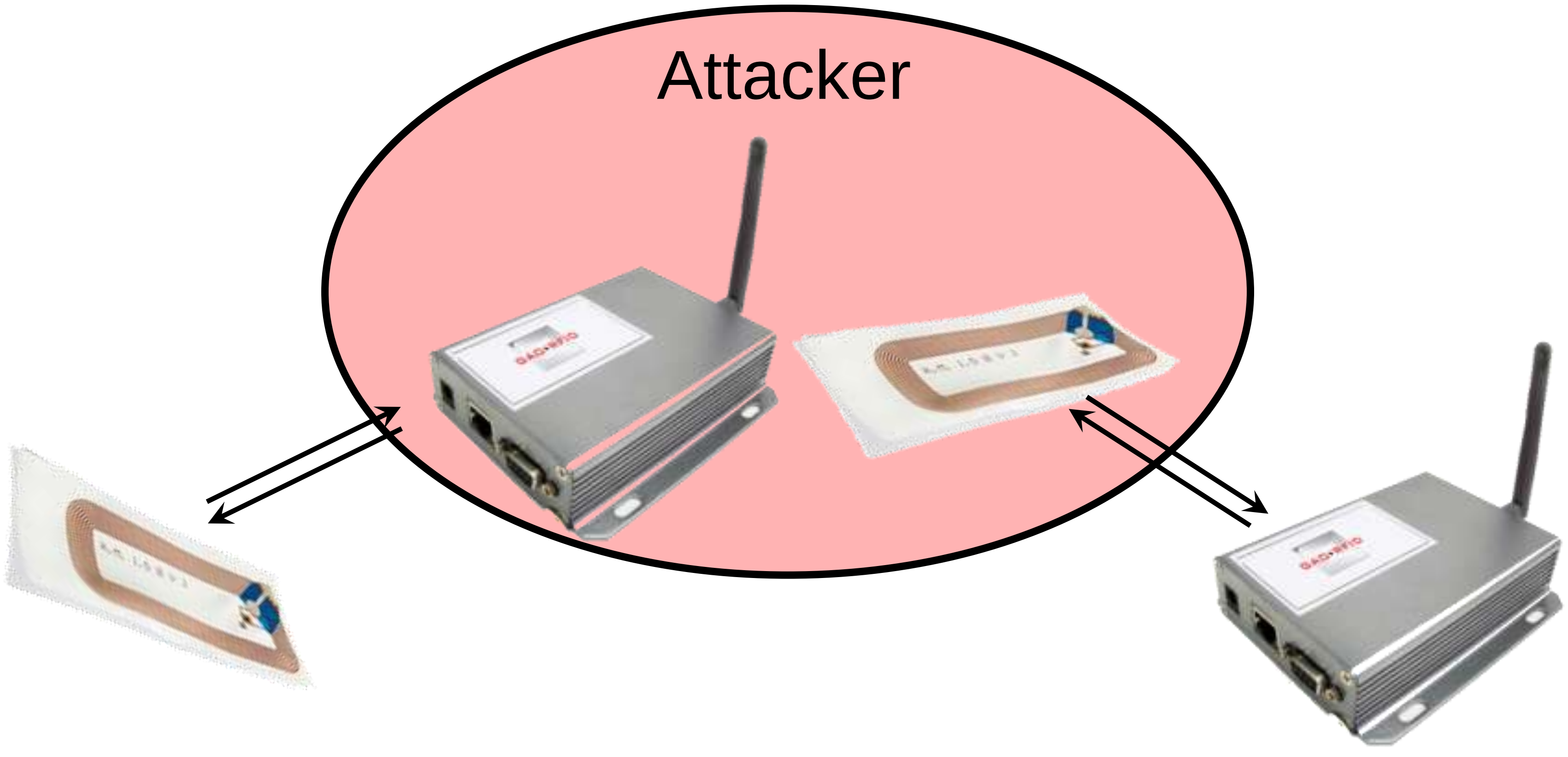


ID, *Rc*

Enc(*Rc*), *Rr*

Enc(*Rr*,*Rc*)

Proxy/Relay Attack



Emulation

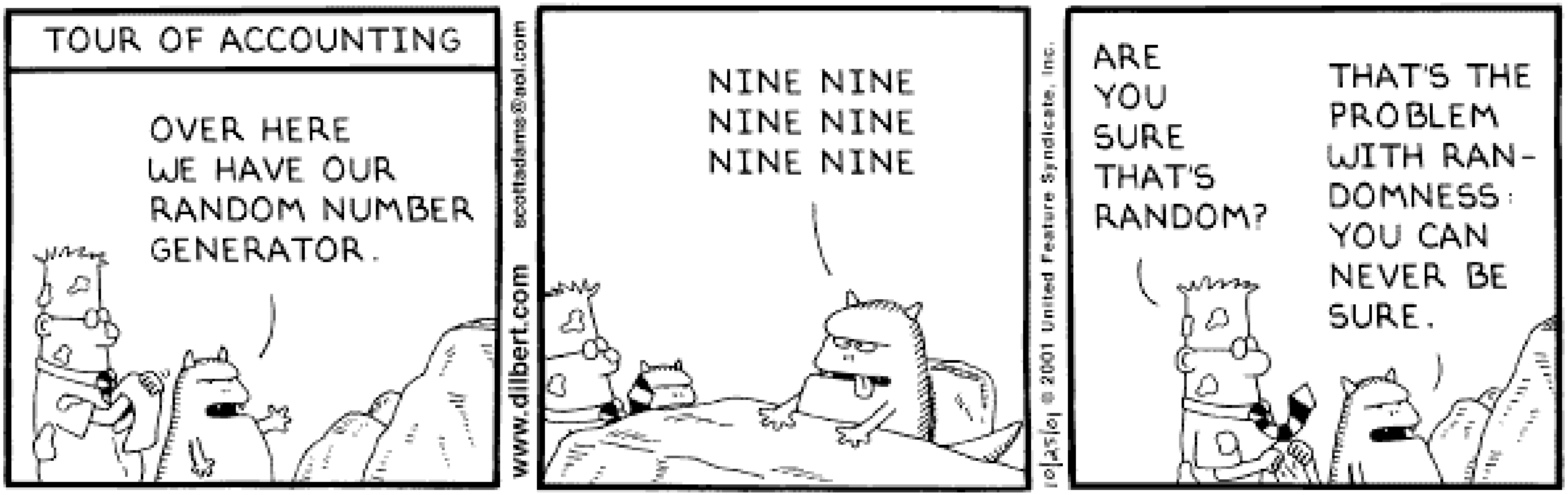
- Spoof “unique” data of tags such as UID
- Done with RFID emulator (OpenPICC) or higher-powered tag (SmartMX)
- Foundation for other attack vectors

Emulation — Mifare

Replay

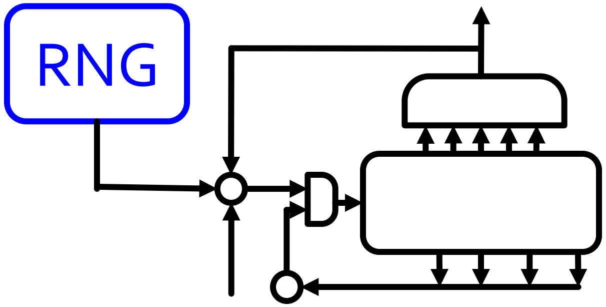
1. Overhear legitimate authentication
2. Force same challenge, answer with same response

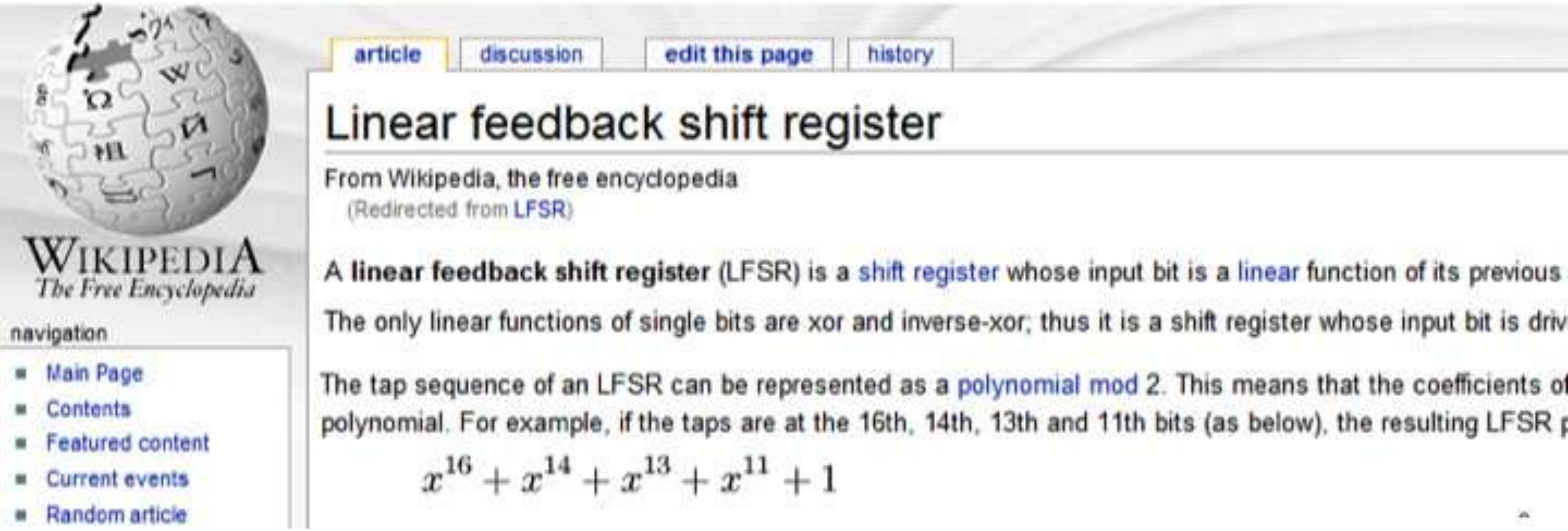
- Requires predictable "random" numbers


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE
10/25/01 © 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

Replay — Mifare

- Mifare random numbers are completely predictable and well documented





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 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

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

Cryptographic Attacks

Recover secret key:

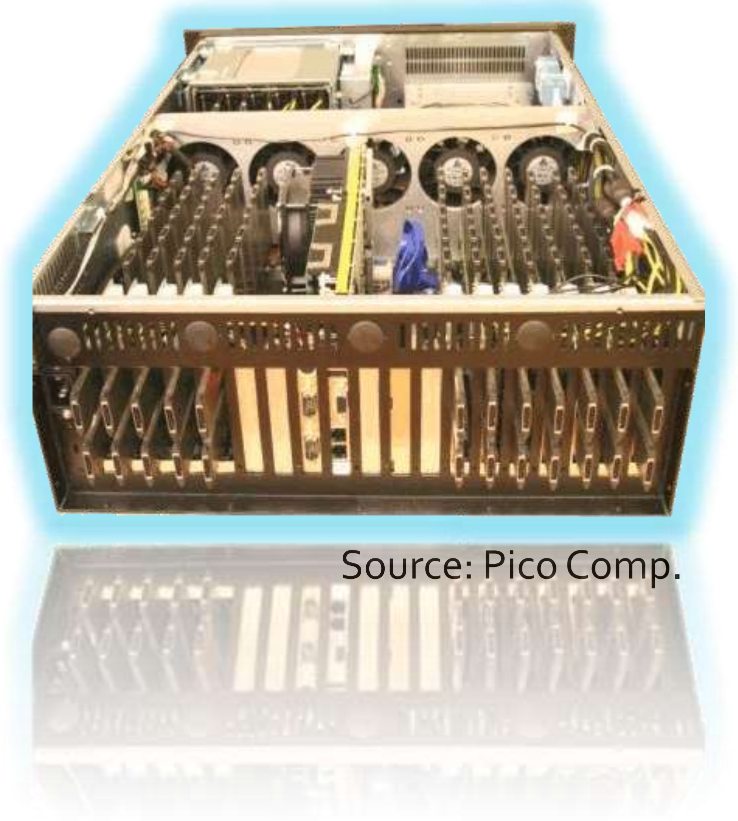
- Brute Force
  - Try all keys
- TMTOs
  - Try all keys, efficiently
- Algebraic Attacks w/ SAT solvers
  - Try all keys, smartly

FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
ÁLÁ'IH, DÓNEH'LINI, DÓNEH'LINI, ÁLÁ'IH, ÁLÁ'IH, DÓNEH'LINI, DÓNEH'LINI, DÓNEH'LINI, ÁLÁ'IH, ÁLAIH, DÓNEH'LINI, ÁLÁ'IH, DÓNEH'LINI, DÓNEH'LINI, DÓNEH'LINI . . .
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

Brute Force Key Search

- "Try all keys"
- Only possible for small keys

- Mifare easy target:
  - Cipher complexity low, enables efficient FPGA implementation
  - FPGA cluster finds key in 50 minutes!



Source: Pico Comp.

Time-Memory Trade-Offs

- Basic idea: Pre-compute and compress code book
- Corner cases:
  - Brute Force: O(N) time
  - Full code book: O(N) space
- Trade offs exists between:
  - Time – space – data/success
- Countermeasure: use IVs

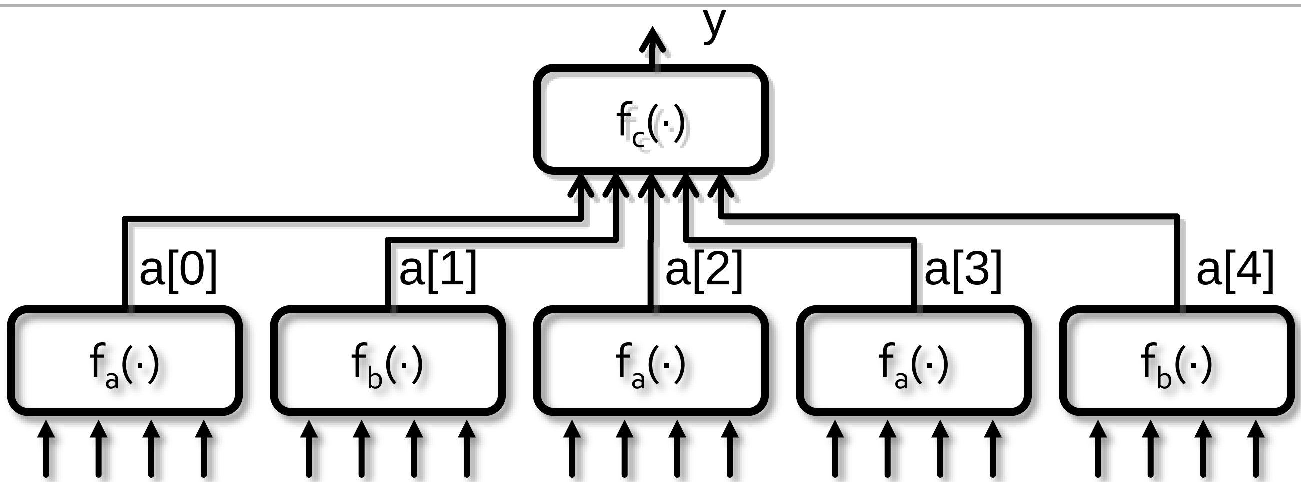
German article "Kunterbuntes Schlüsselraten" on heise.de

Algebraic Attacks

Attacks that exploit simple feedback structure and statistical weaknesses:

1. Describe weak parts of cipher as system of equations
2. Brute-Force through complex parts: *Guess-and-Determine* attack.
3. Solve system of equations: MiniSAT is our friend

Algebraic Attack — Mifare



Compute equations for first output bit:

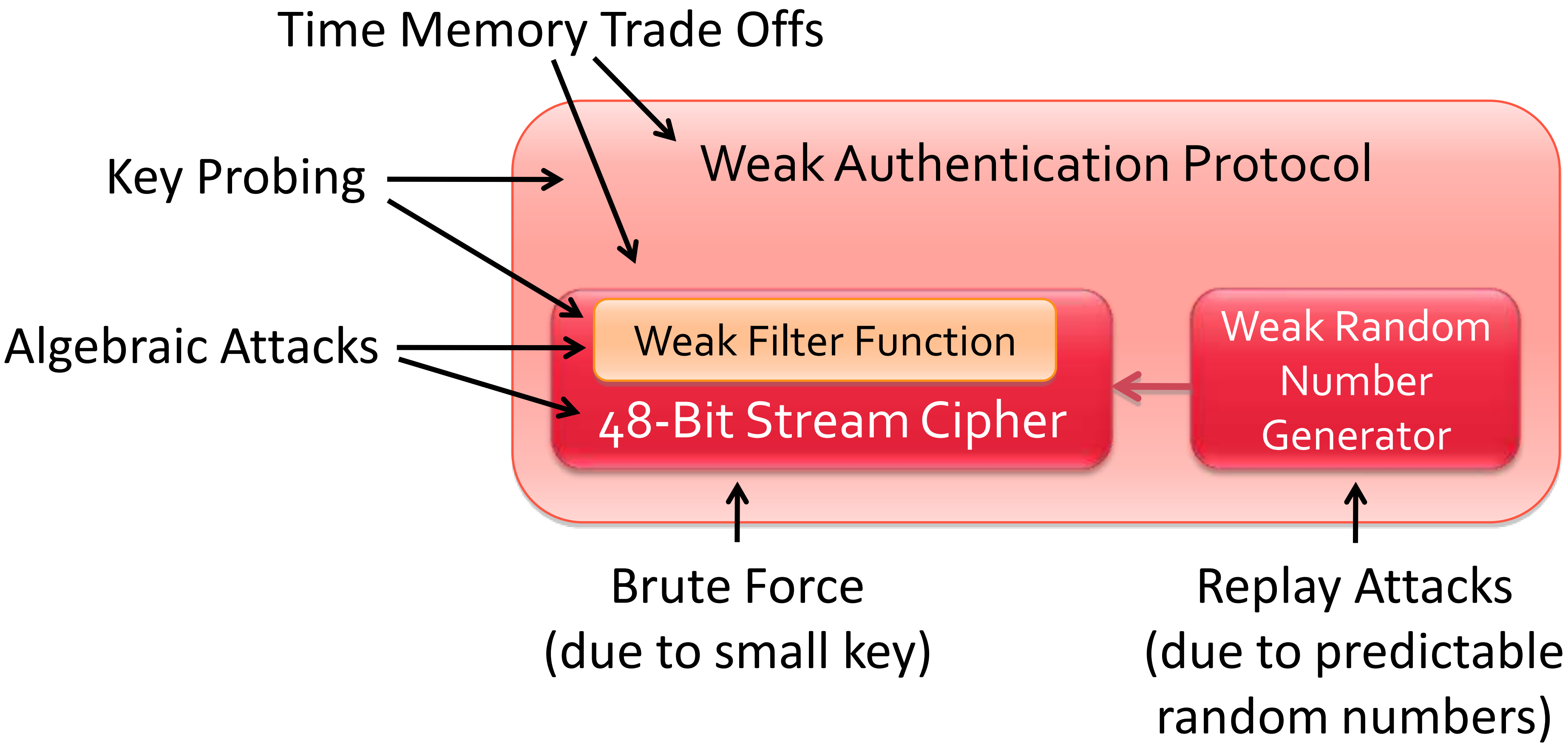
```
a[0] = fa(x[7],x[9],x[11],x[13]);
a[1] = …
…
y    = fc(a[0],a[1],a[2],a[3],a[4])
```

Before computing next bit, shift LFSR:

```
tmp   = x[0]^…^x[43];
for  i=1:47   x[i]=x[i+1];
x[48] = tmp;
```

Describes cipher as system of equations with 48+r⍰5 unknowns, terms with degree ≤ 4!

Mifare Classic Weaknesses



Time Memory Trade Offs

Key Probing

Algebraic Attacks

Weak Authentication Protocol

Weak Filter Function

48-Bit Stream Cipher

Weak Random Number Generator

Brute Force (due to small key)

Replay Attacks (due to predictable random numbers)

Weak Encryption

- Hardware tokens with insufficient security include:
  - Mifare Classic, Hitag2
    - very popular in payment, access control and cars
  - Legic cards (some)
    - popular in access control (Europe)
  - HID cards (some)
    - popular in access control (US)
  - Atmel's secure memory
    - CryptoRF— access control card
    - CryptoMemory—key storage

Source: *hidglobal.com*

Proposed Mitigations

Countermeasures for *Mifare Classic* include:

- Signing:
  - Strongly authenticate data to prove authenticity
  - “Valid states” can be tied to cards and times iff emulation is detectable
- Radio fingerprinting:
  - Measure and verify physical properties of tags
  - Potential to detect emulation
  - (see Day1 talk “RFID fingerprinting” by cryptocrat, Boris Danev)

RFID Tools – TI EVM

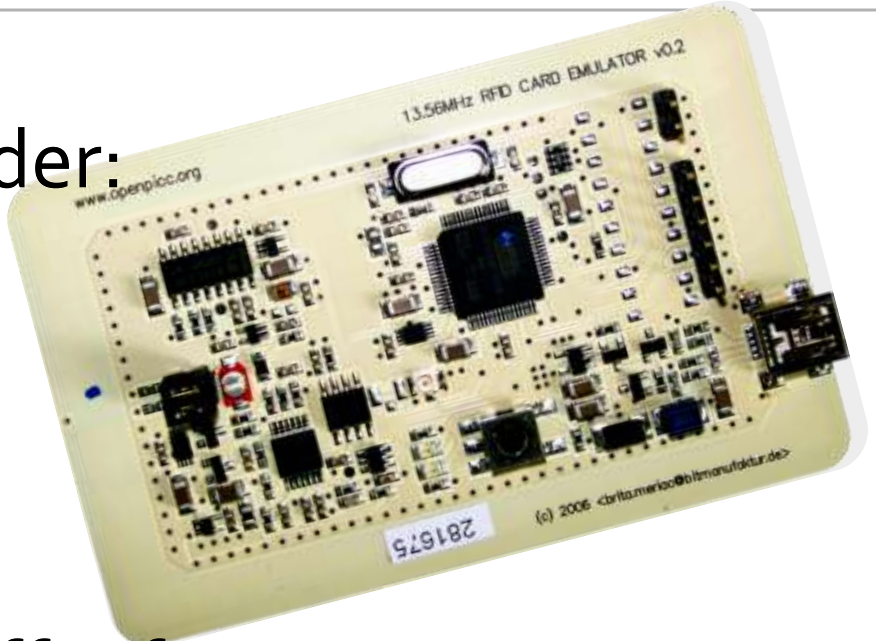
- Multi-protocol, software-extensible RFID kit
- Evaluation module w/ support for Tag-It, ISO 15693, 14443 A/B incl. software-based *Mifare Classic* encryption
- Excellent base for :
  - (upgrade) reader design
  - RFID fuzz tester

Download utility and firmware patch at www.cs.virginia.edu/~kn5f

RFID Tools – OpenPICC Sniffer

Open source RFID tools:

- multi-protocol RFID reader: OpenPCD
- RFID emulator: OpenPICC

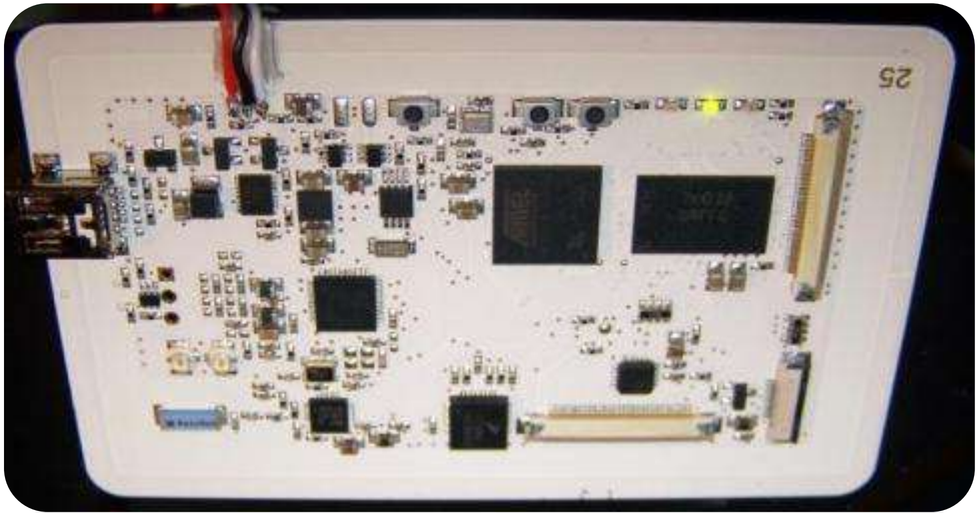

13.56MHz RFID CARD EMULATOR v0.2
www.openpicc.org
281675
(c) 2006 <brita.meriso@bitmanufaktur.de>

- Implemented Mifare sniffer for OpenPICC
  - capture both directions simultaneously
  - sniffing distance: millimeters from card, centimeters from reader

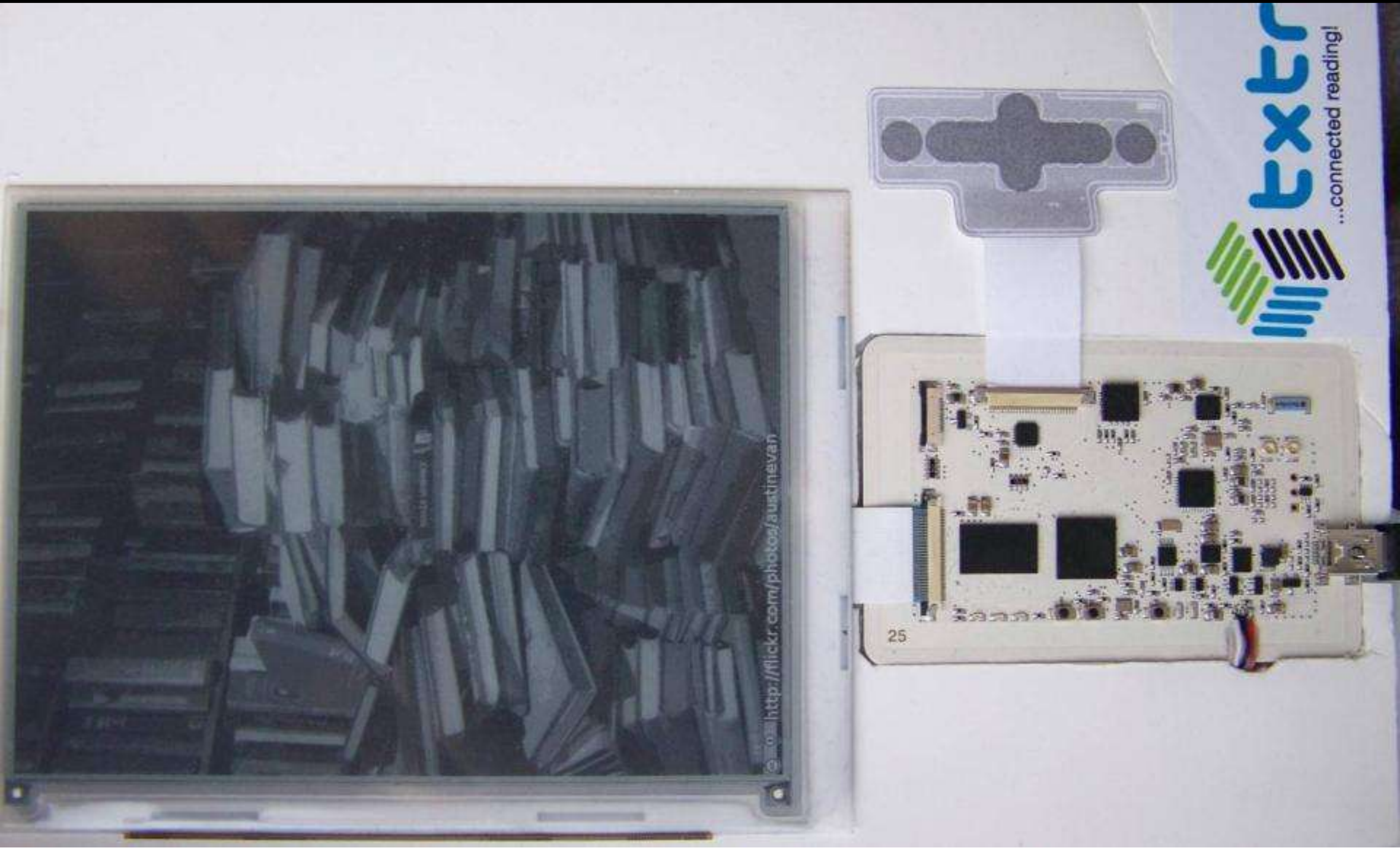
Firmware at svn.openpcd.org/branches/sniffonly/

RFID Tool – OpenPICC2

- Next Generation RFID emulator OpenPICC2:
  - Implements tag and reader side, and OpenBeacon!
  - Sufficient resources for on-board crypto (cracking?):
    - 16 MB Ram, 48 MHz ARM7, SD-card slot
  - Won't be a sniffer, sorry



And it's an eBook reader, too !!!



Take Away

- Use standard protocols and ciphers, but prepare for failure
- Keep hardware upgradable

- We gave you the tools, now start fuzzing, probing, and documenting RFID system
- Join the TI EVM / OpenPICC / OpenPICC2 development efforts
  - Mailing lists on openpcd.org

The Way Ahead

- For secure RFID, we need:
  - Publicly reviewed standards
    - Yes, this means "one-size-fits-all", but requirements are generic
  - Comprehensive threat modeling
    - Threat = risk × damage
  - User engagement, opt-out
    - Never force technology onto users
    - Inform about risks

Questions?

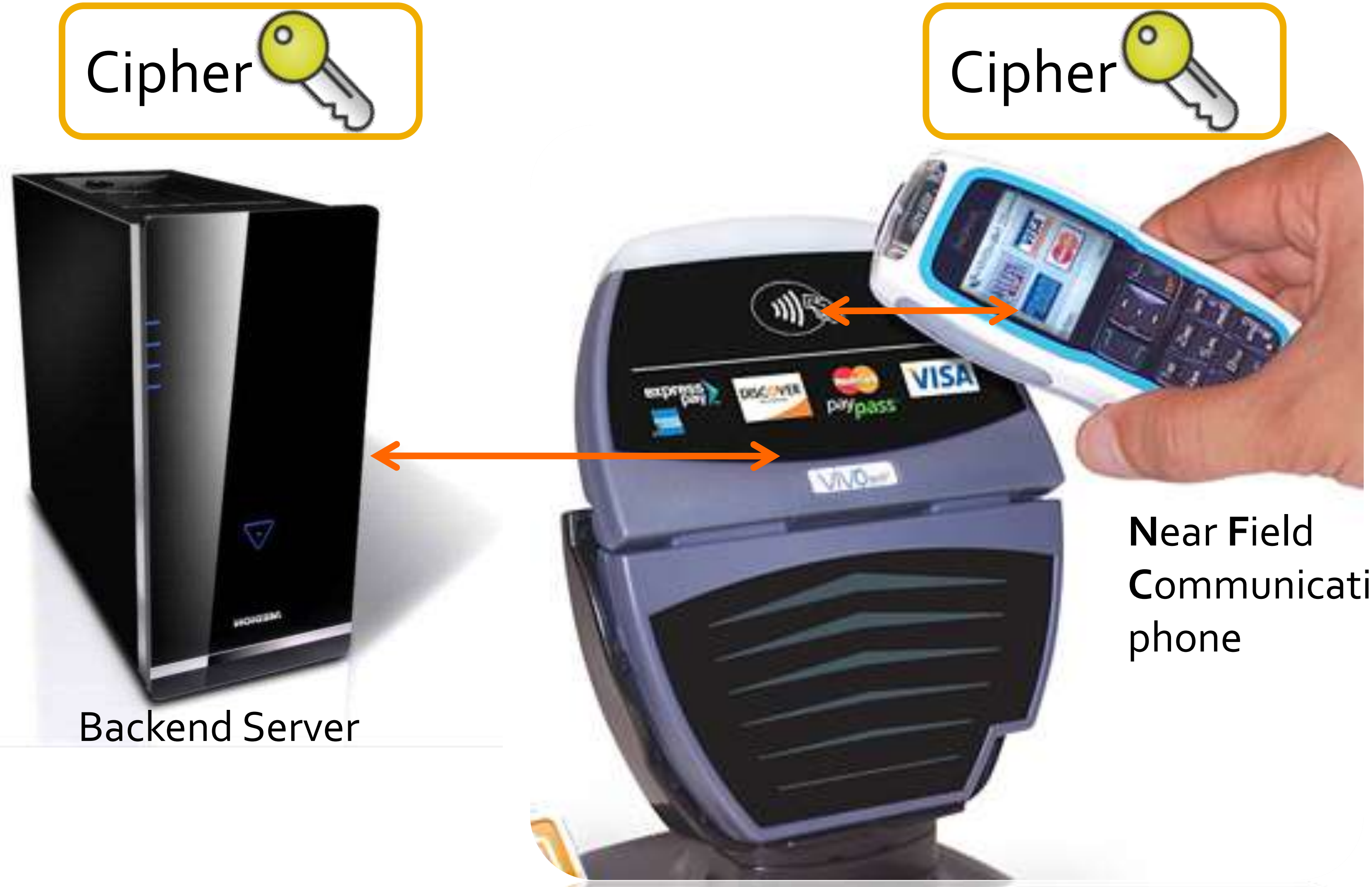
Karsten Nohl
nohl@virginia.edu
Henryk Plötz
ploetz@informatik.
hu-berlin.de

Appendix Slides

Mifare Classic Break

- Mifare cards uses proprietary Crypto-1 algorithm
  - Never publicly reviewed for 20+ years
- We reverse-engineered algorithm and announce insecurities at 24C3
- Feb/Mar: Reports find Crypto-1 to be strong enough for a "few more years"
  - We releases more details about attacks
    - Final report recommends migration
- April: Dutch researchers publicly demonstrate attacks against Oyster
  - Law suit erupts, free speech prevails
  - Details published in October

Example: NFC Payment



Cipher

Cipher

Backend Server

Near **F**ield **C**ommunication phone

Near Field Communication (NFC)

- NFC (=RFID + cell phone) is the next hype
  - Dave Birch: “customers like NFC (a lot)“

> “Most systems are deployed with insufficient security.”

Picture Source: *Collin Mulliner*

NFCs (Lack of) Security

- Jonathan Main, Chair of NFC Technical Committee:

“NFC Forum's role is not to define the [security] requirements [because] a mandatory ‘one-size-fits-all’ approach such as that advocated by Mr. Nohl is not viable.
Many applications use smart card security [...] specified in other consortia. On top of these many security measures, users [can] set their own security parameters and preferences.”

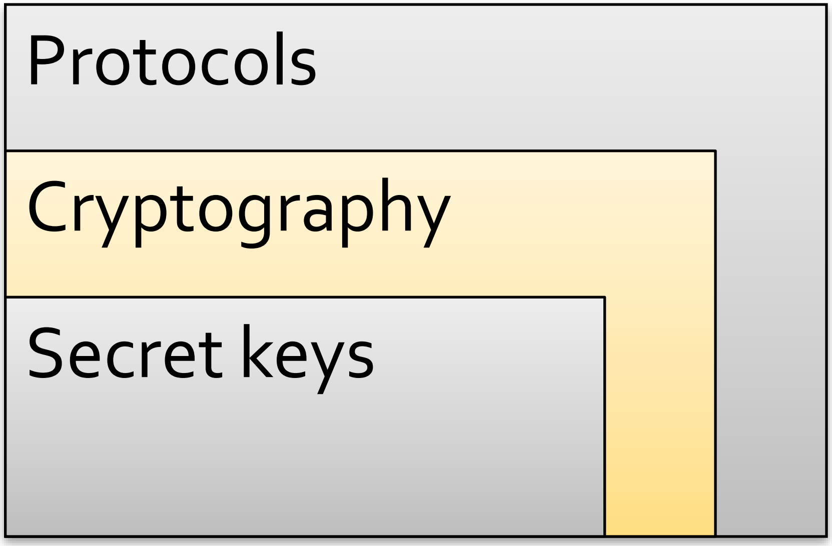
NFC Reality

- The void of standardized security leads to:
  - Development of new proprietary measures
  - Adoption of old, broken security

Often broken protocols,
i.e.: NFC credit cards

Mifare Classic encryption !!

Key storage in insecure SAMs !!!

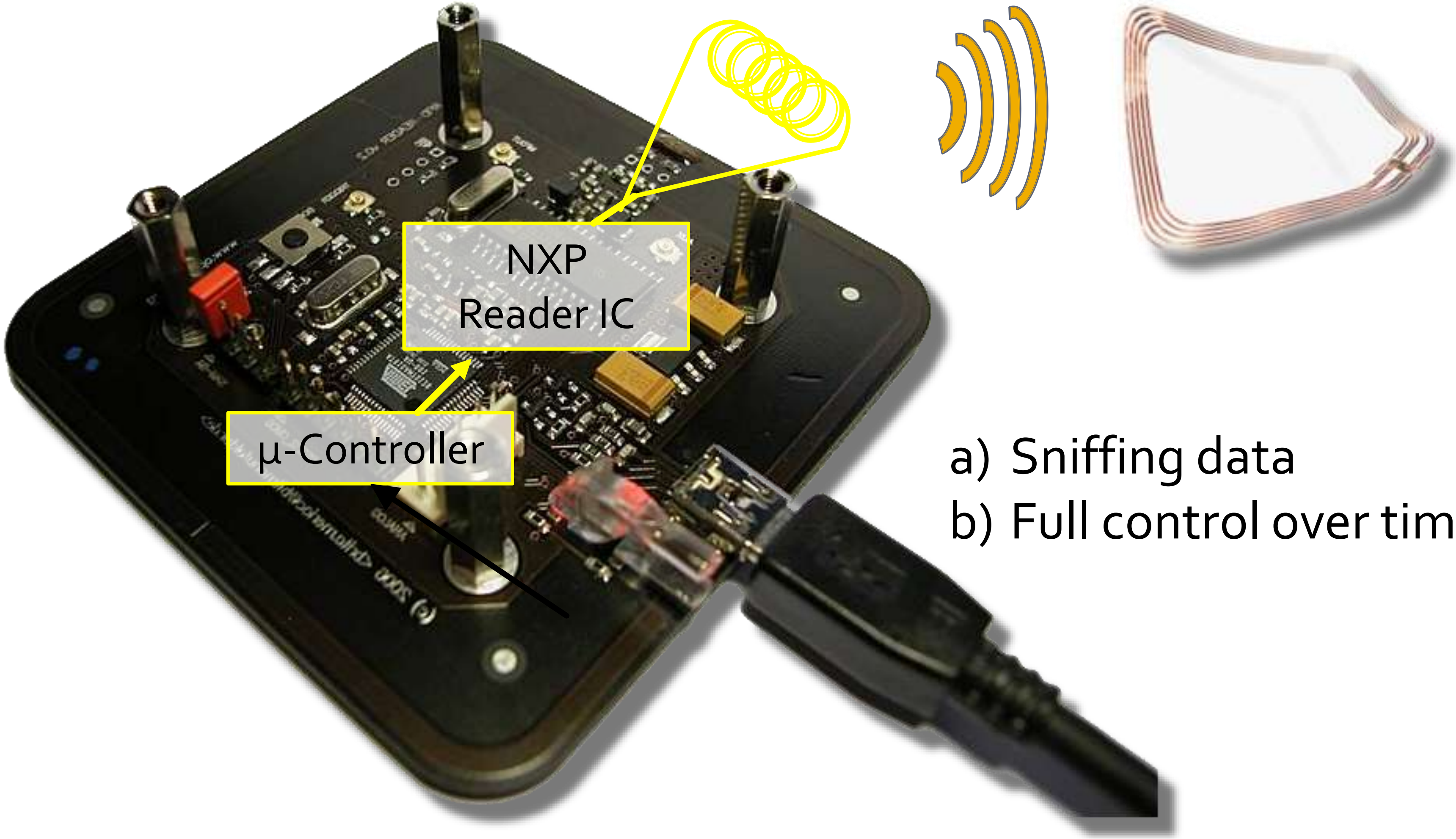


Protocols

Cryptography

Secret keys

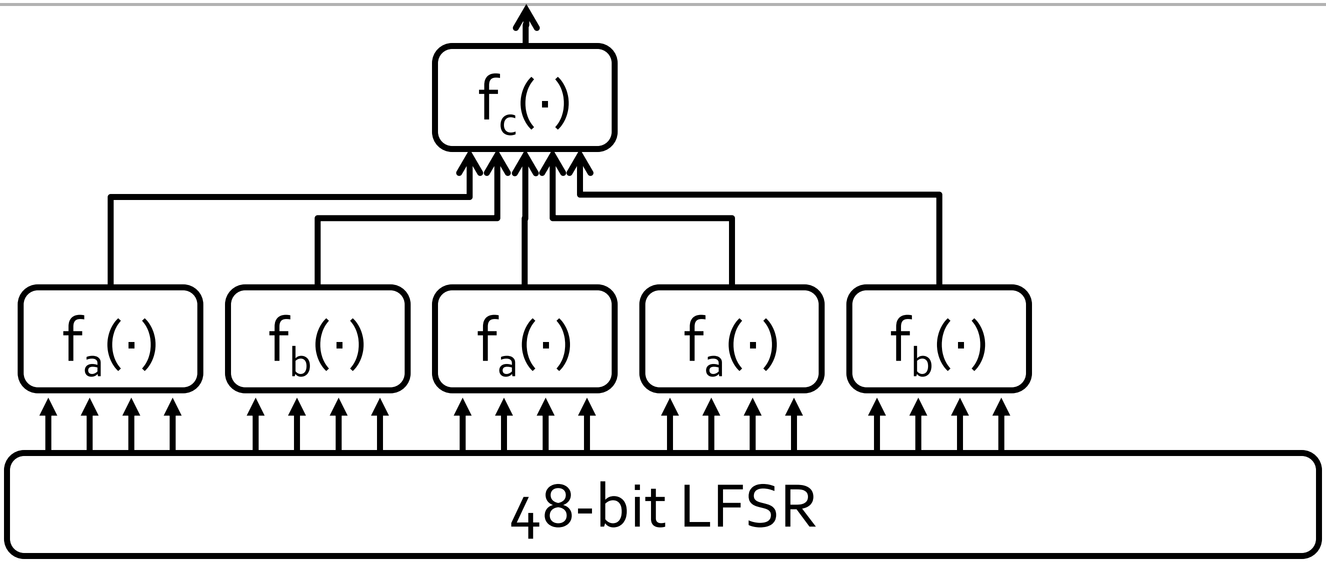
Hardware: OpenPCD (+PICC)



a) Sniffing data

b) Full control over timing!

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
- Finding key takes < 1 minute on laptop