

# Physical Attacks in a Physical World



MIT Cryptography and Information Security Seminar  
June 4, 2010

Christof Paar  
Embedded Security Group  
Ruhr-University Bochum and UMass Amherst

## Acknowledgement

- Thomas Eisenbarth
- Markus Kasper
- Timo Kasper
- Amir Moradi
- David Oswald

## Agenda

---

- Remote Access Control with **KeeLoq**
- Contactless Payments with **Mifare Classic**
- Contactless Smartcards with **3DES**
- Auxiliary Stuff

MIT CIS

## Agenda

---

- **Remote Access Control with KeeLoq**
- Contactless Payments with Mifare Classic
- Contactless Smartcards with 3DES
- Auxiliary Stuff

MIT CIS

## KeeLoq

---

- Introduction to Remote Keyless Entry (RKE) Systems
- Phase 1 – Analysis & Frustration
- Phase 2 – Breakthrough & Euphoria
- Phase 3 – Optimization & Routine

MIT CIS

## KeeLoq

---

- **Introduction to Remote Keyless Entry (RKE) Systems**
- Phase 1 – Analysis & Frustration
- Phase 2 – Breakthrough & Euphorie
- Phase 3 – Optimization & Routine

MIT CIS

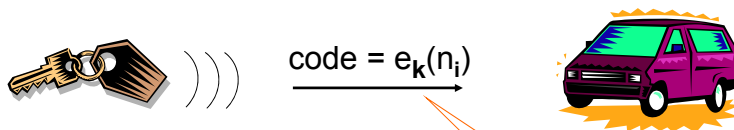
## Remote Keyless Entry Systems



MIT CIS

## Modern Keyless Entry Systems

advanced theft control: rolling code



**rolling code** (or hopping code)  
protects against replay attacks:

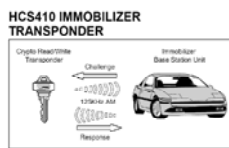
1. code =  $e_k(n)$
2. code =  $e_k(n+1)$
3. code =  $e_k(n+2)$

....

$e_k()$  is often a block cipher

MIT CIS

## Popular RKE Cipher: KeeLoq



- KeeLoq is used in rolling code mode or in a challenge-response protocol
- widely used for **garage doors** in US & Europe
- and for **cars**:  
(Wikipedia: Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Jaguar, ... )
- Several mathematical attacks in 2008 [Bogdanov et al., Indesteege et al., ...]
- ... powerful but still requires  $2^{16}$  plaintexts

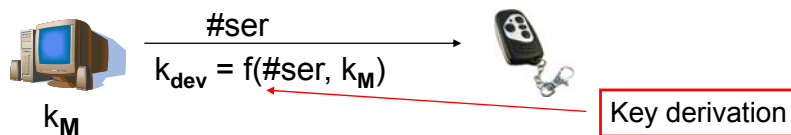
Q: Will physical attacks work better?

MIT CIS

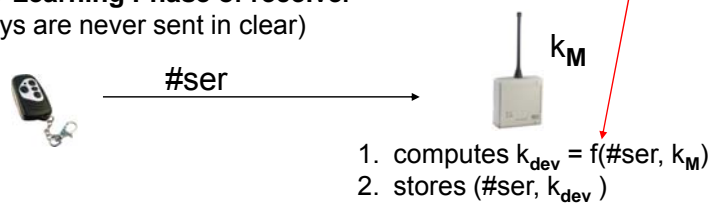
## Key Management

### 1. Creation of new remote (in secure environment)

OEM has 1 *manufacturer key*  $k_M$  (burned in all its receivers)



### 2. Key Learning Phase of receiver (keys are never sent in clear)



MIT CIS

## KeeLoq

- Introduction to Remote Keyless Entry (RKE) Systems
- **Phase 1 – Analysis & Frustration**
- Phase 2 – Breakthrough & Euphoria
- Phase 3 – Optimization & Routine

MIT CIS

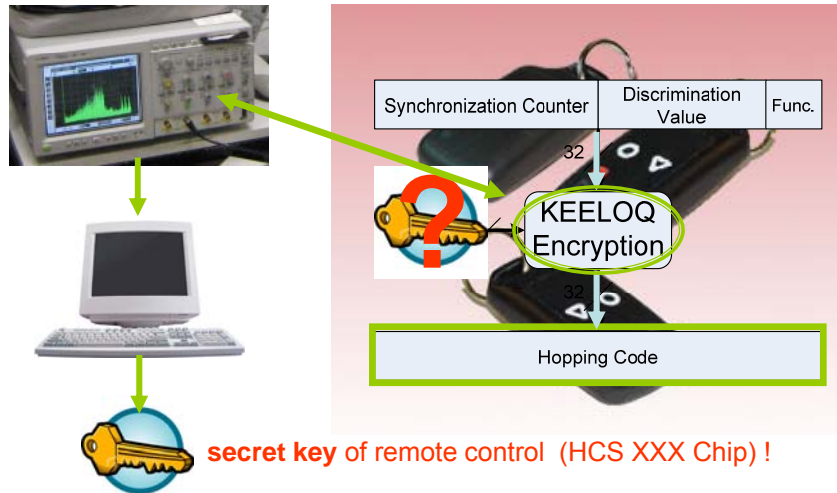
## KeeLoq + Side-Channel Attacks

Our thoughts ca. 2006 (mostly correct)

- Great target for real-world attack ✓
- Old cipher ✓
- Implementation probably also 10+ years old ✓
- SCA countermeasures very unlikely ✓
- Running DPA or SPA should be a piece of cake (a few weeks) † † †

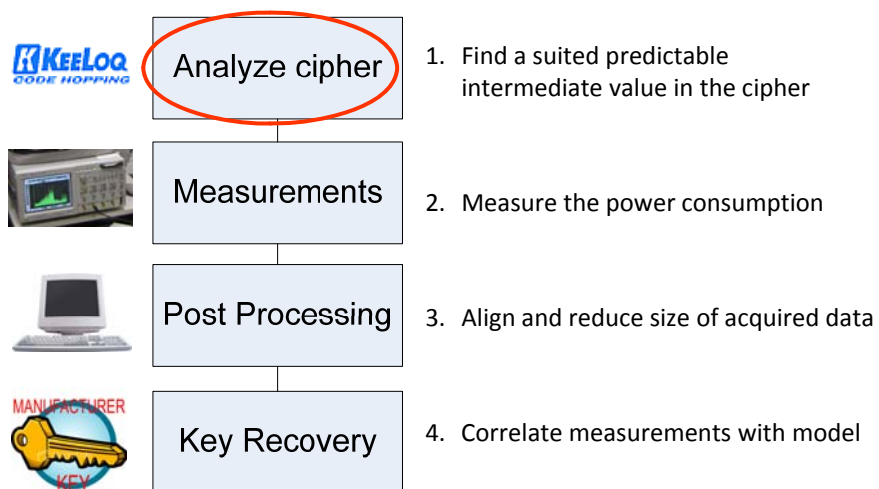
MIT CIS

## Power Analysis of a Remote Control



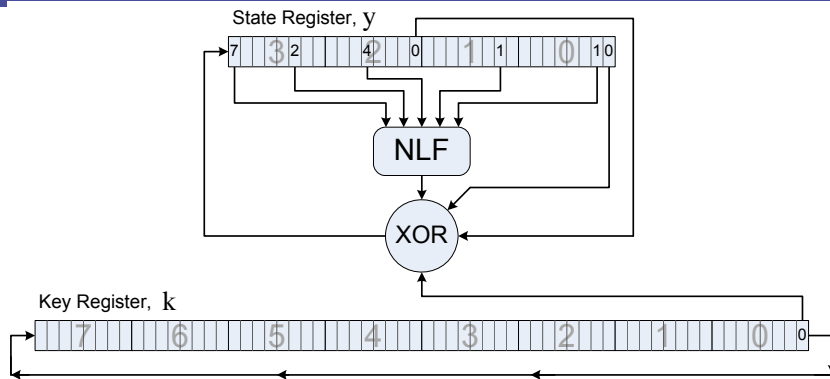
MIT CIS

## Performing the Side-Channel Attack



MIT CIS

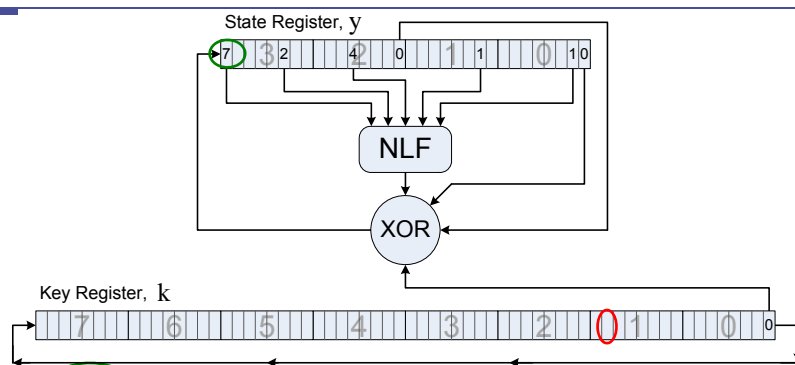
### KeeLoq – Algorithm



- 64 bit key, 32 bit block length
  - NLFSR comprising a 5x1 non-linear function
  - Simple key management: key is rotated in every clock cycle
  - 528 rounds, each round one key bit is read
- Lightweight cipher – cheap and efficient in hardware

MIT CIS

### KeeLoq – Attack



$$y_{31}^{(i+1)} = k_0^{(i)} \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus \text{NLF} \left( y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)} \right)$$

$$y_0^{(527)} = k_{15}^{(527)} \oplus y_{16}^{(527)} \oplus y_{31}^{(528)} \oplus \text{NLF} \left( y_{31}^{(527)}, y_{26}^{(527)}, y_{20}^{(527)}, y_9^{(527)}, y_1^{(527)} \right)$$

→ knowing the state directly reveals one key bit per clock cycle

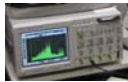
MIT CIS

## Performing the Side-Channel Attack



Analyze cipher

1. Find a suited predictable intermediate value in the cipher



Measurements

2. Measure the power consumption



Post Processing

3. Align and reduce size of acquired data



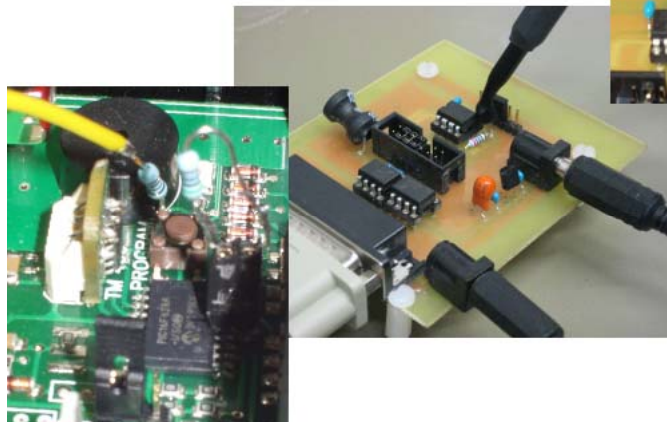
Key Recovery

4. Correlate measurements with model

MIT CIS

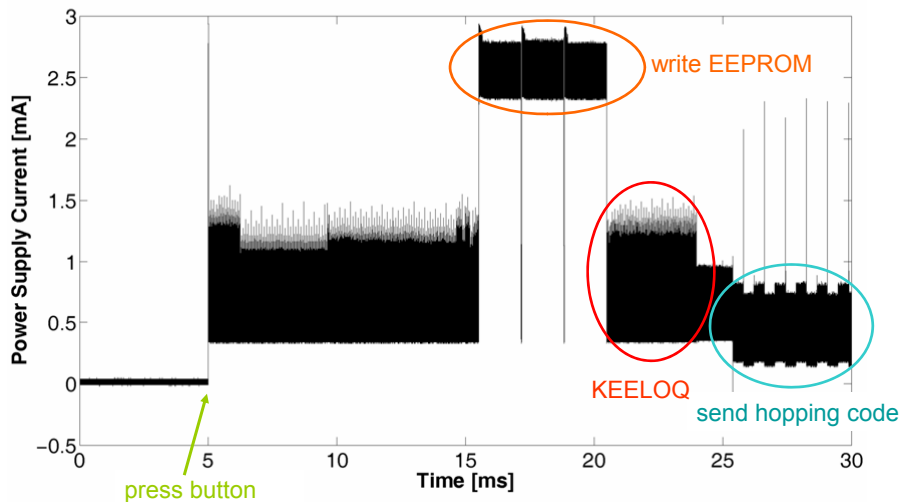
## Measuring the Power Consumption

- Digital oscilloscope (max. 1 GS/s sample rate)
- Measure electric current or electromagnetic field



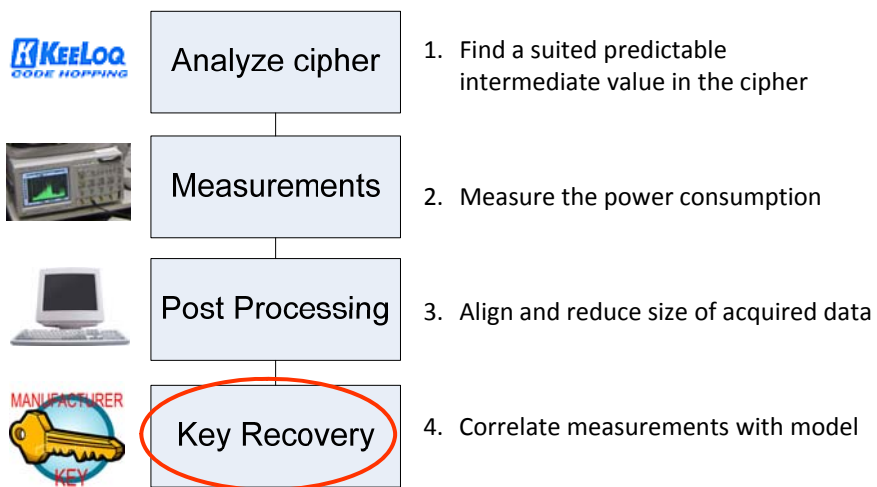
MIT CIS

## Power Trace of a remote control: Finding the KEELOQ - Encryption



MIT CIS

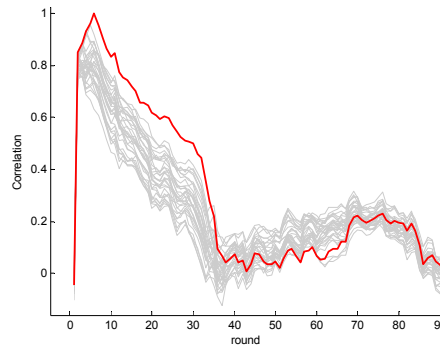
## Performing the Side-Channel Attack



MIT CIS

## Performing the Side-Channel Attack Key Recovery

- Correlate real power consumption  $I_i$  with predicted value  $D = f(X_i, K_h)$
- Divide-and-conquer approach
- Best-matching key candidates “survive”



$$r(I_i(t), D(X_i, K_h)) = \frac{\sum_{i=1}^M I_i(t) \cdot D(X_i, K_h)}{\sqrt{\sum_{i=1}^M (I_i(t) - \overline{I_i(t)})^2 \cdot \sum_{i=1}^M (D(X_i, K_h) - \overline{D(X_i, K_h)})^2}}$$

$$= \frac{\frac{1}{M} \cdot \sum_{i=1}^M I_i(t) \cdot \sum_{i=1}^M D(X_i, K_h)}{\sqrt{\sum_{i=1}^M (I_i(t) - \overline{I_i(t)})^2 \cdot \sum_{i=1}^M (D(X_i, K_h) - \overline{D(X_i, K_h)})^2}}$$

MIT CIS

## KeeLoq

- Introduction to Remote Keyless Entry (RKE) Systems
- Phase 1 – Analysis & Frustration
- **Phase 2 – Breakthrough & Euphoria**
- Phase 3 – Optimization & Routine

MIT CIS

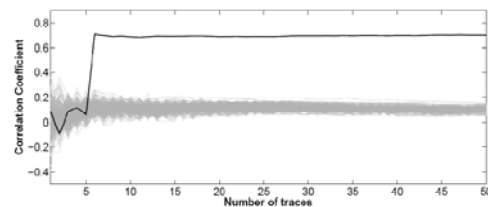
... 15 months later

MIT CIS

### Side-Channel Attack Results for KeeLoq

A) Hardware implementation (“car key”)

- Total attack time (for known device family):  
5-30 traces,  $\approx$  minutes



B) Software implementation (“car door”)

- Total attack time (for known device family):  
1000-5000 traces,  $\approx$  hours
- reveals Manufacturer Key for ALL key derivation modes

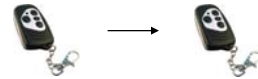


MIT CIS

## So what can we do now (1) ?

1. If we have access to a remote:

Recover Device Key and clone the remote



2. If we have access to a receiver:

Recover Manufacturer Key & generate new remotes

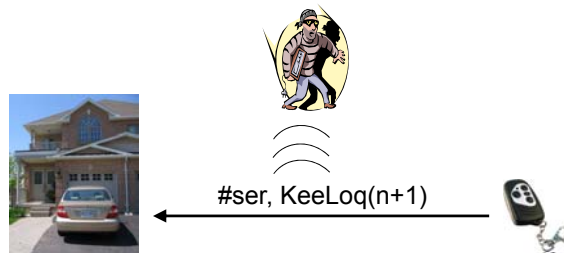


MIT CIS

## So what can we do now (2) ?

After extracting of manufacturing key:

**Remotely eavesdrop on 1-2 communications & clone key!**



- works for all key derivation schemes
- might require a few hours of computation (Rem: not necessary for any system we've analysed.)
- SCA attack is not specific to KeeLoq, e.g., unprotected AES is vulnerable too.

**! Side-channel step (recovery of manufacturer key, difficult) can be outsourced to criminal cryptographers !**

## KeeLoq

---

- Introduction to Remote Keyless Entry (RKE) Systems
- Phase 1 – Analysis & Frustration
- Phase 2 – Breakthrough & Euphoria
- **Phase 3 – Optimization & Routine**

## After the Attack

---

3 reactions from industry

1. Companies ignore us (many)
2. Companies hate us (also popular)
3. Companies want to improve their products with us (few)

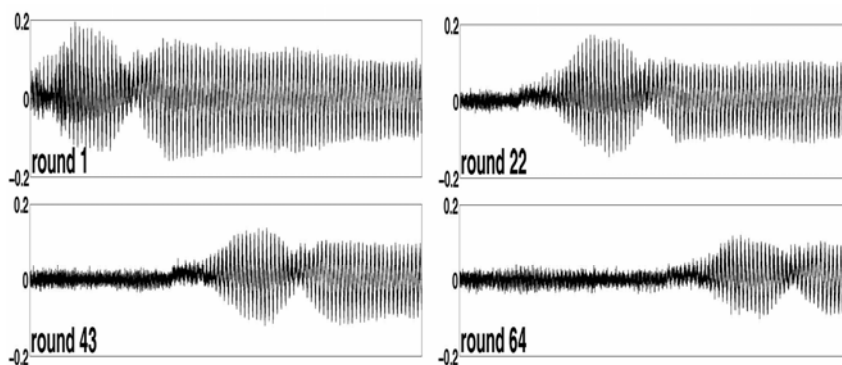
## Since 2008

- We analyzed several KeeLoq products
- All are breakable
- But efforts for manufacturing key recovery varies from hours ... weeks
- We gained much experience and started to improve ...

MIT CIS

## Recall: Software DPA needs 1000s of Measurements

Correlation for DPA decreases with #rounds (bad)



Duration of one round seems to be dependent on input  
→ **good** for SPA !

## KeeLoq Decryption Program Code

```

; DECRYPT using [Key7 . . . Key0]
; | HOP4 | HOP3 | HOP2 | HOP1 | <-- Feed

DECRYPT
00: MOVW 11+1 ; OUTLOOP COUNTER
01: MOVWF CNT1 ; 11+1 TIMES

OUTLOOP
02: MOVW 48 ; INLOOP COUNTER
03: MOVWF CNT0 ; 48 TIMES

INLOOP
04: CLRWDI ;
05: MOVWF CNT1 ;
06: XORLW 1 ;
07: SKPZS ; LAST 48 LOOPS
08: GOTO ROT_KEY ; RESTORE THE KEY

09: CLAC ; CLEAR CARRY
0A: MOVW 1 ; MASK = 1
0B: BTFSC HOP3,3 ; SHIFT MASK 4X
0C: MOVW 10000B ; IF BIT 2 SET
0D: MOVWF MASK ;

0E: BTFSS HOP2,0 ; SHIFT MASK
0F: GOTO $+3 ; ANOTHER 2X
10: RLF MASK ; IF BIT 1 SET
11: RLF MASK ;

12: BTFSC HOP1,0 ; SHIFT MASK
13: RLF MASK ; 1X MORE IF BIT 0

14: MOVW 0 ; TABLE INDEX = 0
15: BTFSC HOP4,1 ; IF BIT 3 SET
16: XORLW 2 ; TABLE INDEX ** 2
17: BTFSC HOP4,6 ; IF BIT 4 SET
18: XORLW 4 ; TABLE INDEX ** 4

19: ADDWF PC ; PC ** TABLE INDEX

TABLE
1A: MOVW 02EH ; BITS 4:3 WERE 00
1B: GOTO T_END ; END OF TABLE

1C: MOVW 074H ; BITS 4:3 WERE 01
1D: GOTO T_END ; END OF TABLE

T_END
1E: MOVW 05CH ; BITS 4:3 WERE 10
1F: GOTO T_END ; END OF TABLE

20: MOVW 03AH ; BITS 4:3 WERE 11

T_END
21: ANDWF MASK ; ISOLATE THE
22: MOVW 0 ; CORRECT BIT
23: SKPZ ;
24: MOVW 80H ; W = NLF OUTPUT

25: XORWF HOP2,W ; W XOR= HOP2,7
26: XORWF HOP4,W ; W XOR= HOP4,7
27: XORWF KEY1,W ; W XOR= KEYREG1,7

28: MOVWF MASK ; FEEDBACK = BIT 7
29: RLF MASK ; CARRY = BIT 7

3A: RLF HOP1 ; SHIFT IN
3B: RLF HOP2 ; THE NEW BIT
3C: RLF HOP3 ;
3D: RLF HOP4 ;

ROT_KEY
2E: CLAC ; CLEAR CARRY
2F: BTFSC KEY7,7 ; IF BIT 7 SET
30: SETC ; SET CARRY

31: RLF KEY0 ; LEFT-ROTATE
32: RLF KEY1 ; THE 64-BIT KEY
33: RLF KEY2 ;
34: RLF KEY3 ;
35: RLF KEY4 ;
36: RLF KEY5 ;
37: RLF KEY6 ;
38: RLF KEY7 ;

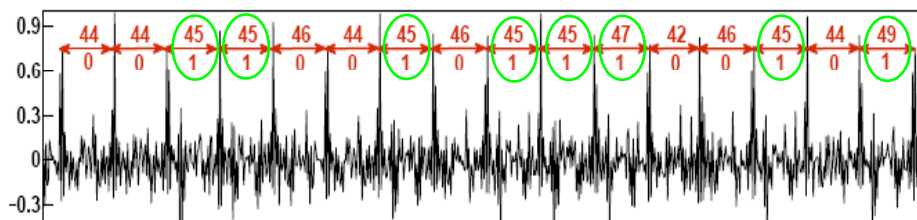
39: DECFZS CNT0 ;
3A: GOTO INLOOP ; INLOOP 48 TIMES

3B: DECFZS CNT1 ;
3C: GOTO OUTLOOP ; OUTLOOP 12 TIMES

3D: RETLW 0 ; RETURN
    
```

Data dependent code  
in red

## Round-time depends on key bit!



44, 46 clocks → key bit = 0  
 45, 47, 49 clocks → key bit = 1

→ allows SPA attack!

## KeeLoq and SPA: What can we do now?

- Manufacturing key recovery with **1 single power trace**
- No need to profile the leakage (unlike template attacks)
- Countermeasure: fix execution time of rounds  
But: Better alignment of traces will make DPA easier ...
- Further details: our Crypto 08 and Africacrypt 09 papers

Important lesson

Do not educate your attacker, i.e., build rock solid systems from the beginning.

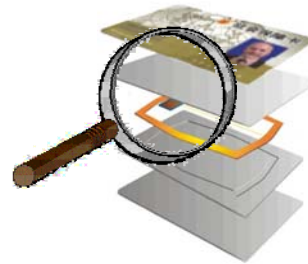
MIT CIS

## Agenda

- Remote Access Control with KeeLoq
- **Contactless Payments with Mifare Classic**
- Contactless Smartcards with 3DES
- Auxiliary Stuff

MIT CIS

## How secure are practical contactless payment systems? Let's investigate one large-scale system !



- contactless employee ID card, e.g., of a large corporate enterprise
- more than 1 million users according to the manufacturer
- **payment card (cafeteria, printing, ...)**, access control, ...
- Based on *Mifare Classic 1K* chip



MIT CIS

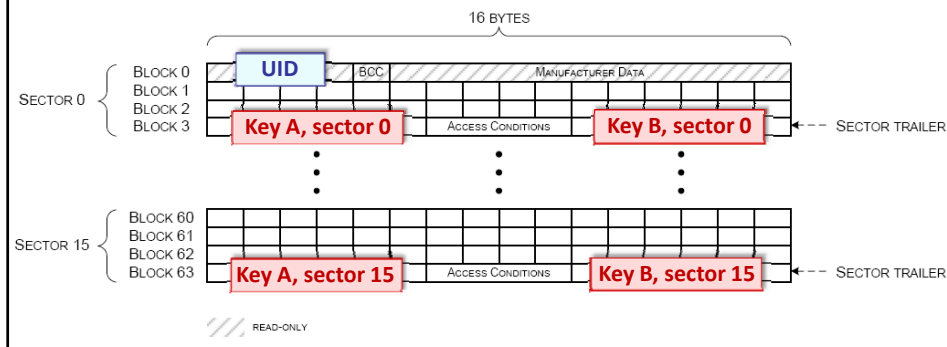
## Mifare Classic and its Security

MIT CIS

## Mifare Classic 1K

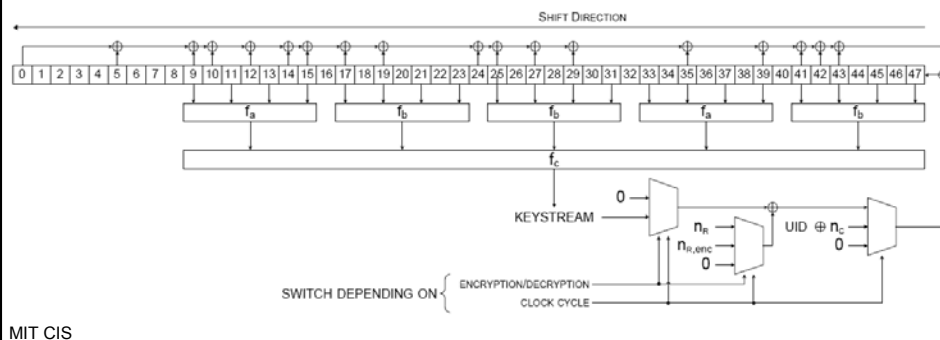


- “more than 1 billion“ cards used worldwide, e.g, for public transport
- contactless memory card with simple encryption, cheap ( $\approx 0,50$  €)
- each card contains a factory-programmed, read-only **Unique Identifier (UID)**
- access to each sector can be secured with **two cryptographic keys A and B**

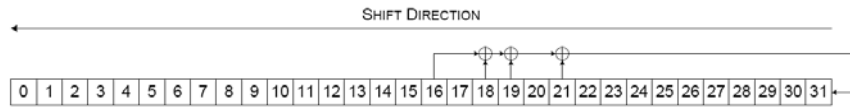


## 1. Weakness: Outdated Cipher

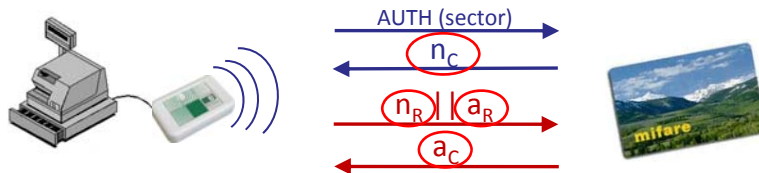
- proprietary **stream cipher CRYPTO1** since early 1990s
- cipher reversed engineered ca. 2008 [Nohl et al]
- several severe flaws found [Garcia et al, Courtois]  
→ small cipher state, weak non-linear functions



## 2. Weakness: Poor RNG

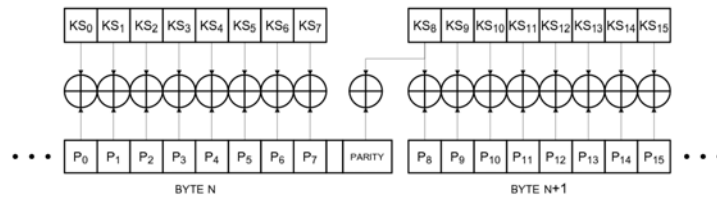


- generates 32-bit nonces  $n_x$  and responses  $a_x$  for the authentication
- only 16 bit instead of possible 32 bit
- “randomness” depends only on the time elapsed since power-up !



MIT CIS

## 3. Weakness: Bad Protocol



- bad practice: **keystream bits reused**
- **parity calculated over plaintext** instead of actually transmitted data
- bug/feature: card replies with 4 encrypted bits (NACK = 0x05), if the parity bits for the encrypted  $n_R || a_R$  are correct, but  $a_R$  is wrong \*  
 → can be used as **covert channel to recover parts of the keystream**

\*) guess parity bits: 1 out of  $2^8$  tries will be successful

MIT CIS

## Analyzing a Real World Contactless Payment System

MIT CIS

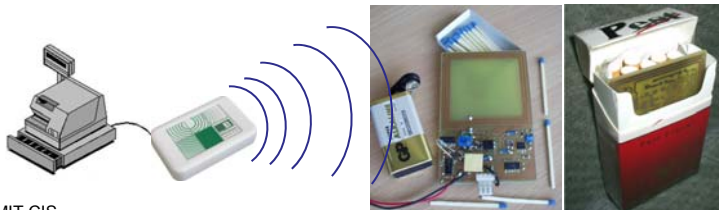
### Special RFID Tools



**Special Reader:** Precise control of the timing (accuracy: 75 ns)  
→ **FIX** the the card's random nonce to exactly **one value!**

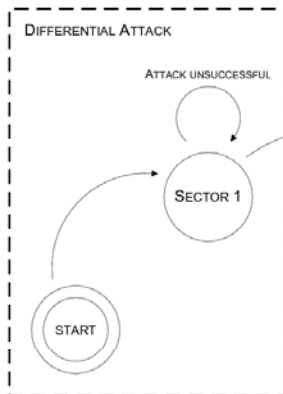


**Fake Tag:** Can completely emulate any ISO14443 transponder  
(e.g., Mifare cards) **including an arbitrary UID**



MIT CIS

## Our Combined Attack

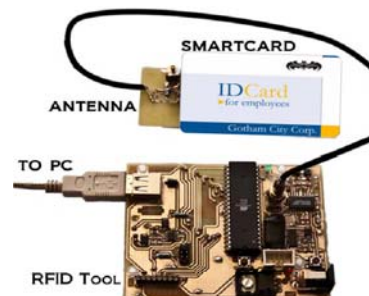


1. differential attack [Courtois] to extract the 1<sup>st</sup> secret key
  2. nested authentication attack for the remaining keys
- ! **card nonce fixed** to exactly one value !
- **recover all keys of a Mifare 1K card in < 10 min**

MIT CIS

## Analysis of the ID-Card 1/2

- test our attack on ID-Card of employe #1  
→ extraction of all secret keys
- try ID-Card of employee #2  
→ card contains the *same* keys
- try ID-Card of employee #3  
→ card contains the *same* keys
- ...
- → Happy attackers: all ID-Cards use **identical keys**



MIT CIS

## Analysis of the ID-Card 2/2

1. **one-time** extraction of the secret keys of **any** ID-Card  
*duration: < 10 minutes*



2. reverse-engineering of the **card's content** (repeated „pay-and-compare“ )
  - **card number**: integrity "ensured" with XOR checksum (UID&card number)
  - **credit balance**: **€ in plain** w/o any protection
  - **other data**: date of card issuance, last payment terminal, ...
3. knowing the above: **wireless** manipulation of **all** cards in the system from **10 ... 25 cm** (depending on antenna) within **milliseconds**

MIT CIS

## Impersonation Attack: Duplicate an ID-Card

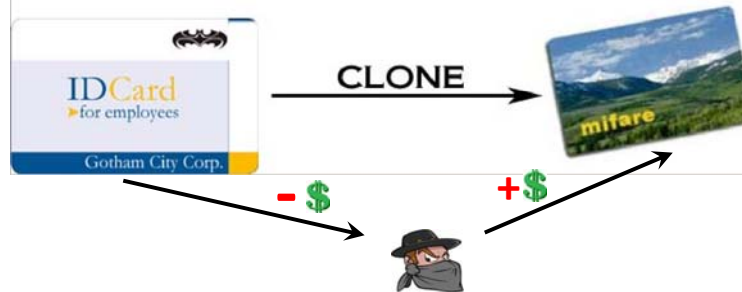


- contactless read-out of relevant data in 100 msec
- copy content of victim's ID-Card to blank Mifare Classic (eBay: < 0,50 € )
- card number and credit balance remain unchanged
- alternatively: increase balance

→ pay with a duplicate of a card that appears "legitimate" to the system

MIT CIS

## Impersonation Attack (variant): Wireless Pickpocketing

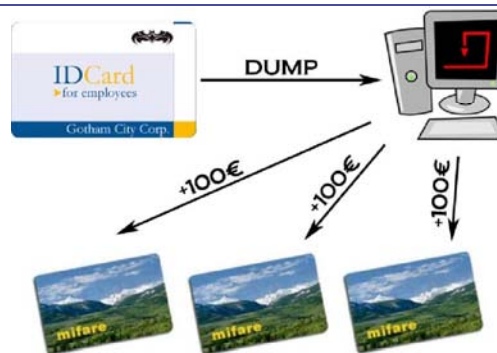


- attacker in addition **lowers the credit on the victim's card**
- advantage: perhaps difficult to detect (no additional money in the system)

→ **direct loss for the victims,**  
**no net loss for the payment institution**

MIT CIS

## Selling Pre-Charged Cards

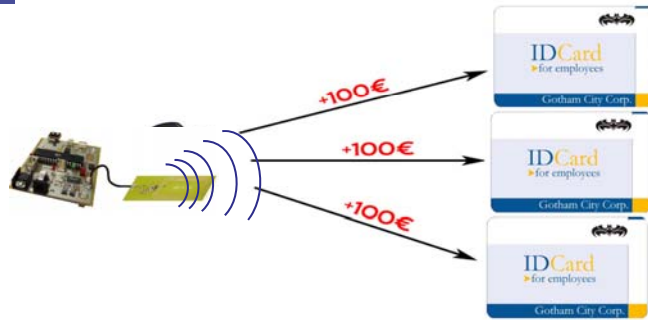


- dump the content of a valid ID-Card to a PC
- generate new card number and write to new (blank) card
- optionally: modify credit balance
- sell the cards (say, 1€ for card with 10€ balance)

MIT CIS



## Distributed All-You-Can-Eat



- disguised reader, **charges** cards of “victims”
- system shut-down likely, even with low penetration rate

### Remarks:

- *Ethics*: Who will you complain about a free 100€ voucher?
- *Legal*: Can you be sued for s.o. else charging your card?

MIT CIS

## Summary of the Analyses

- Mifare attacks even more efficient than anticipated
- also more devastating than anticipated
- In addition to an outdated cipher: numerous flaws in the system design (e.g., no functioning shadow accounts)
- unfortunately this is not a single occurrence
- Owner of the system almost entirely clueless, system integrators (techies!) also surprisingly un-knowledgeable
- Details: our Financial Crypto '09 paper

MIT CIS

## Agenda

---

- Remote Access Control with KeeLoq
- Contactless Payments with Mifare Classic
- **Contactless Smartcards with 3DES**
- Auxiliary Stuff

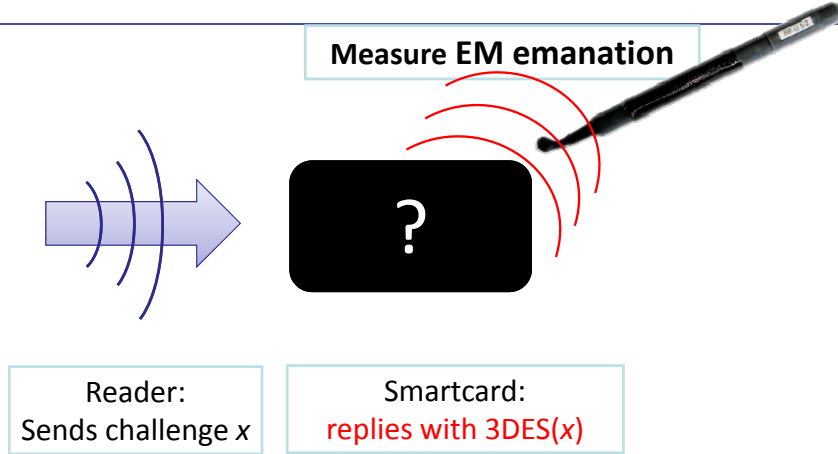
MIT CIS

## Let's step back for a minute ...

---

- OK, KeeLoq and Mifare Classic are insecure
- Congratulations: You can break 1980s ciphers with current techniques.
- What about DESfire, a 3DES contactless card?

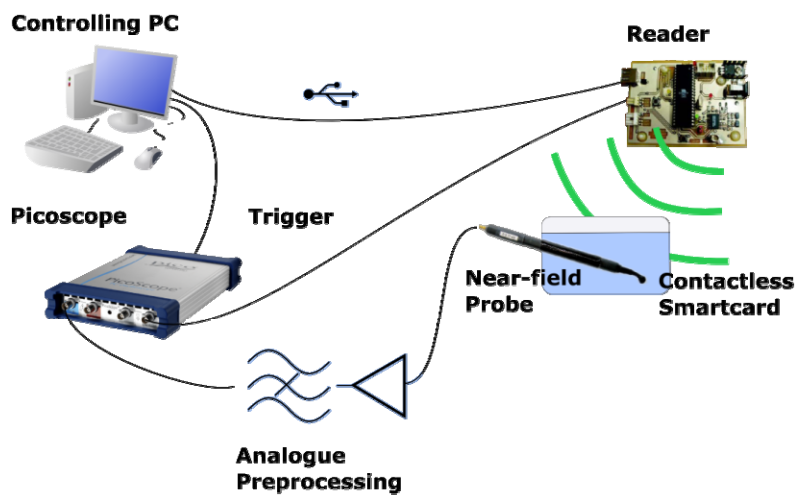
### Basics: Side-channel measurements of contactless smart cards



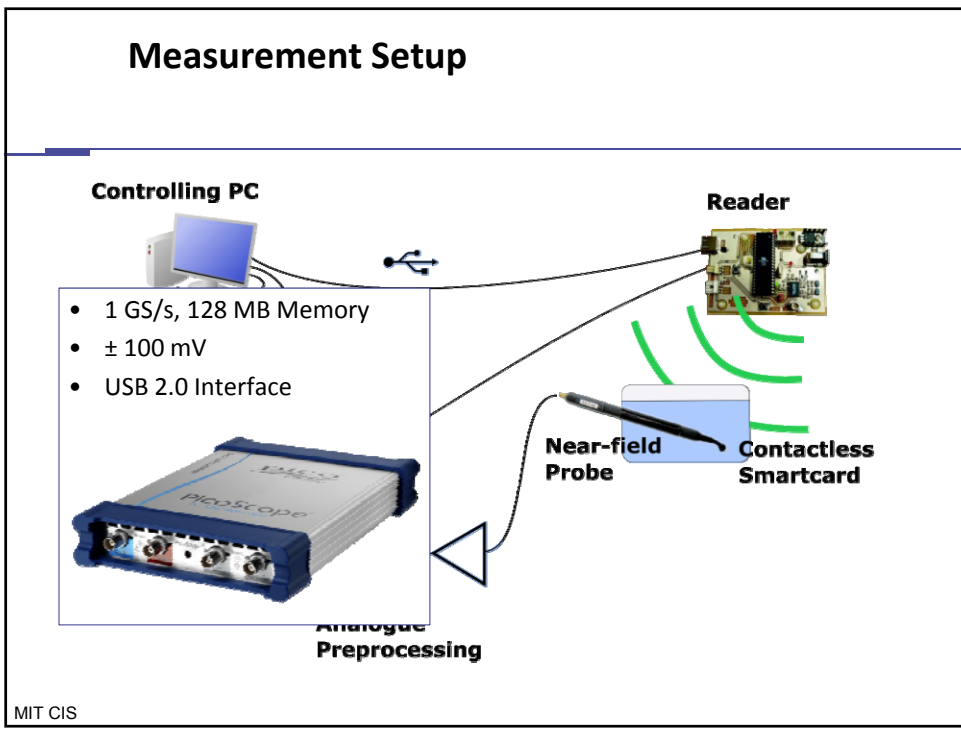
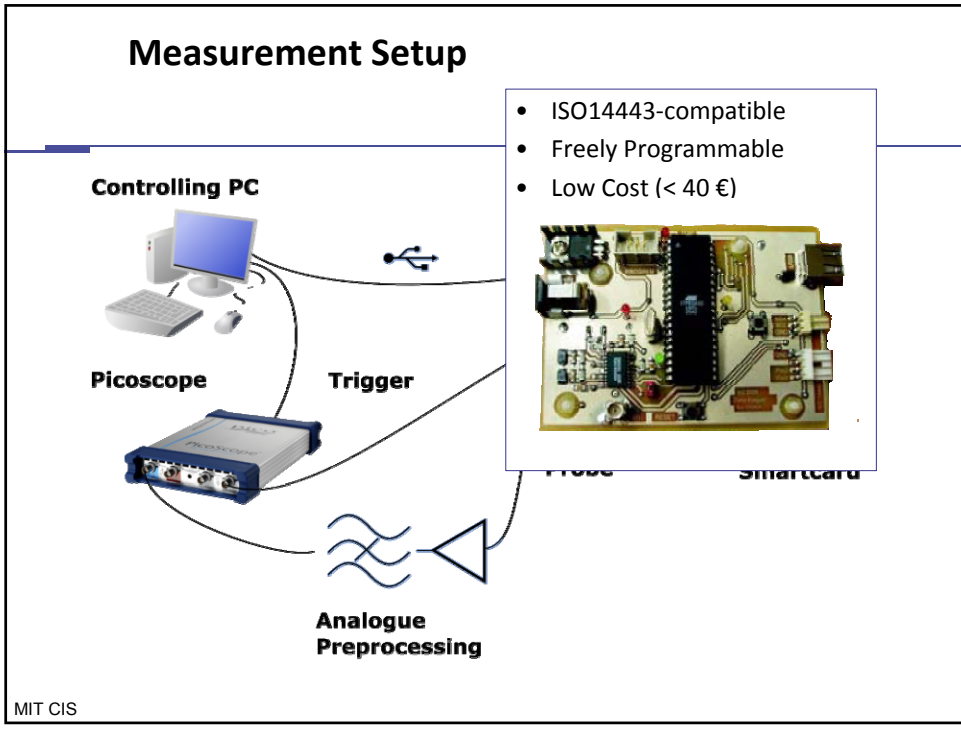
- strong EM field of reader prevents straightforward DEMA

MIT CIS

### Measurement Setup



MIT CIS



## Measurement Setup

Controlling PC



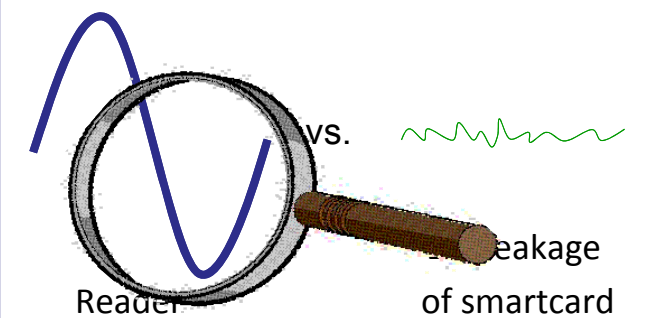
Reader



Picoscope



Aim: Reduce Carrier Wave Influence



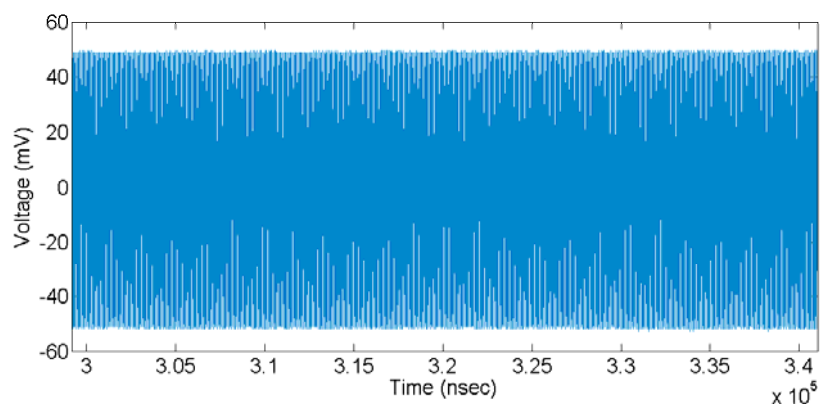
MIT CIS

## Side Channel Analysis

Step 1: Raw measurements

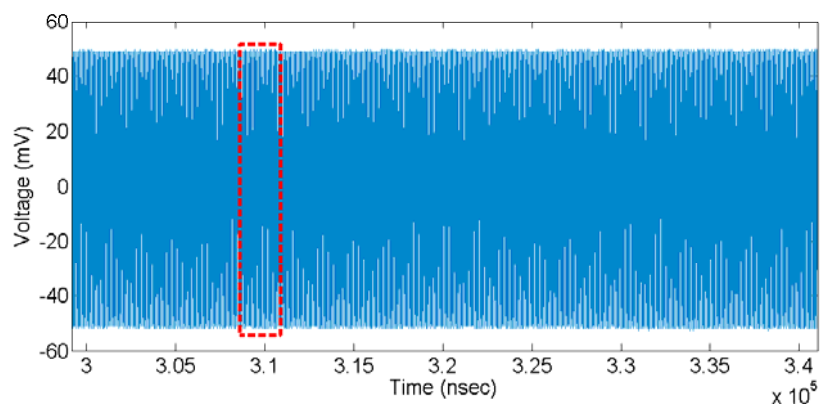


### EM Trace (without analog filter)



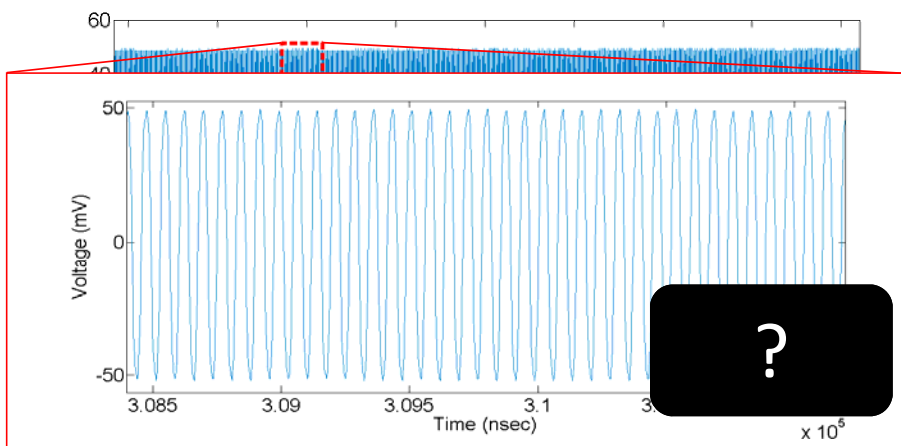
MIT CIS

### EM Trace (without analogue filter)



MIT CIS

### EM Trace (without analog filter)

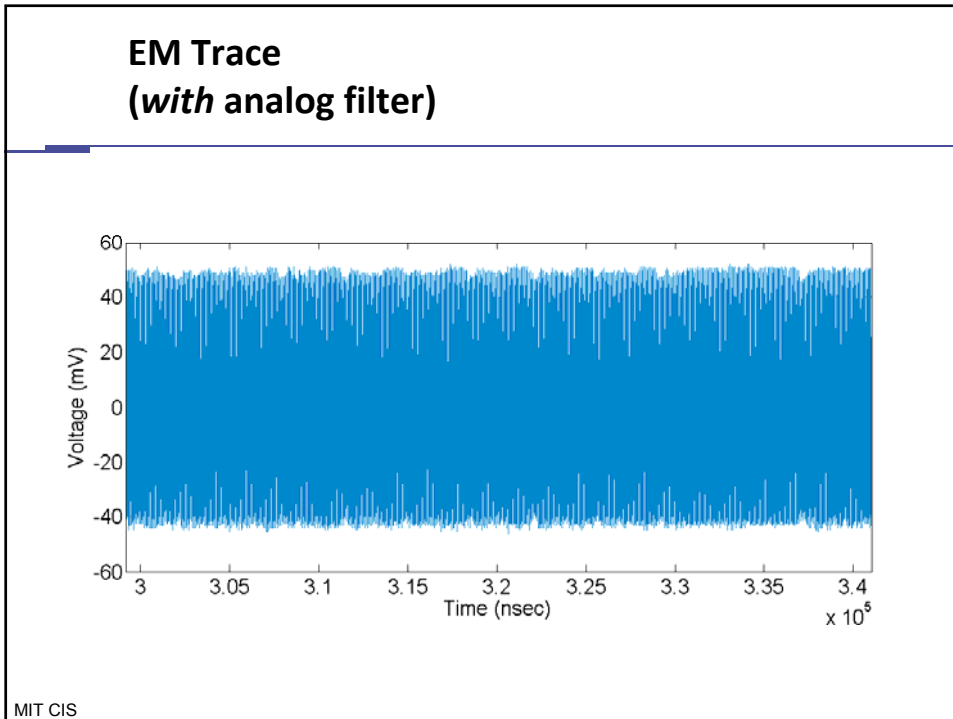
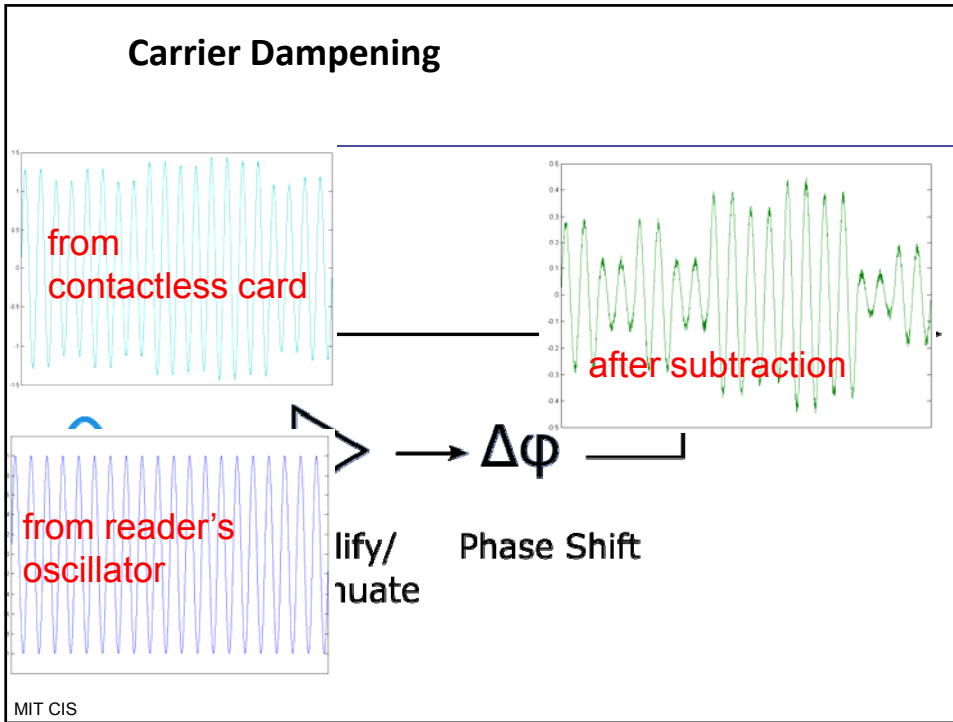


MIT CIS

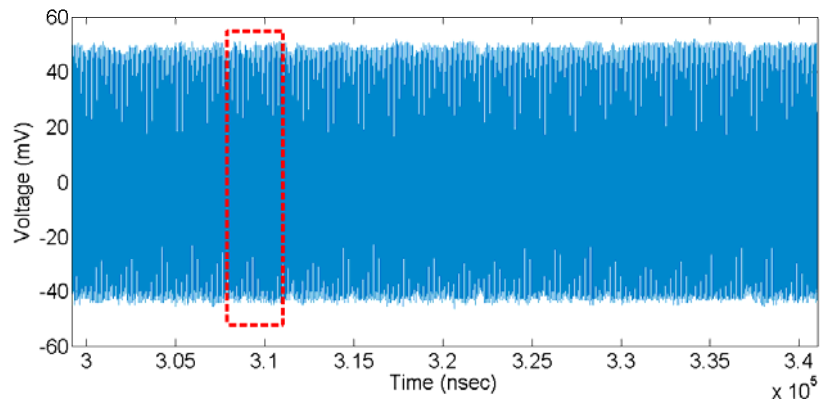
### Side Channel Analysis

#### Step 2: Analog filter



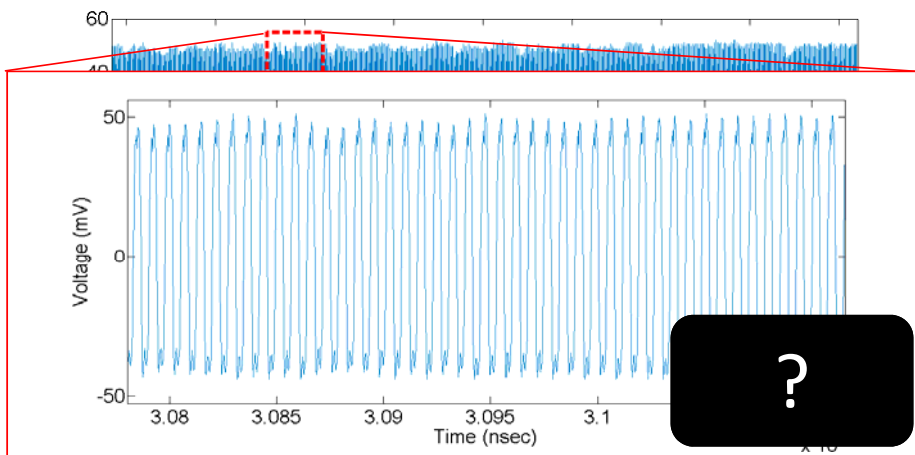


### EM Trace (with analogue filter)



MIT CIS

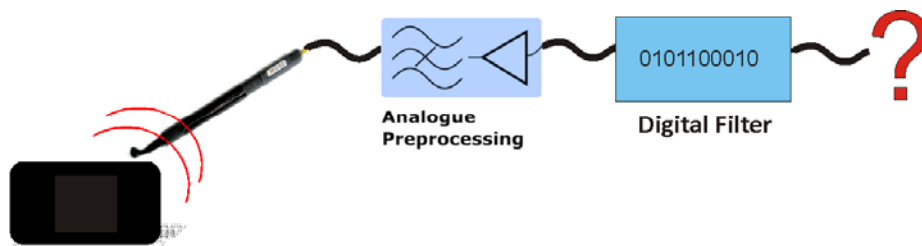
### EM Trace (with analogue filter)



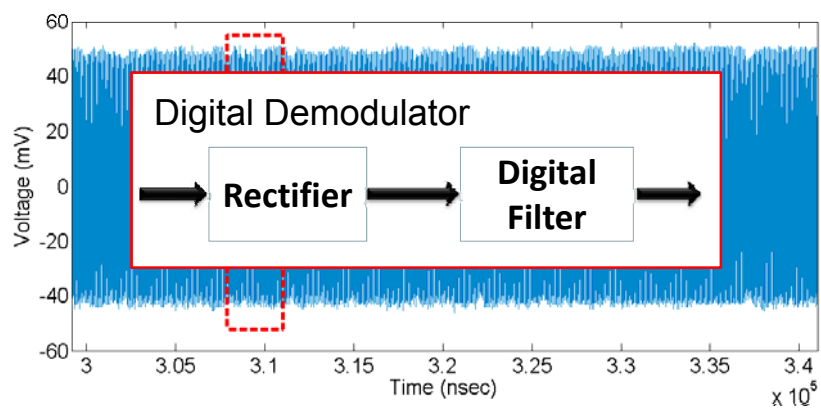
MIT CIS

## Side Channel Analysis

### Step 3: Digital Demodulation

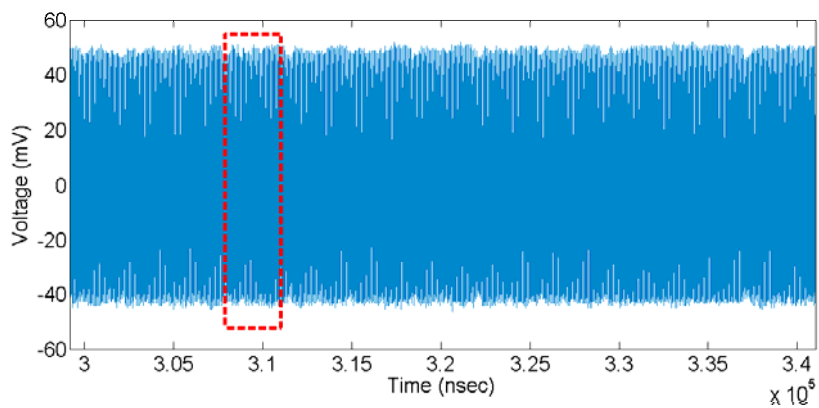


### Digital Demodulation



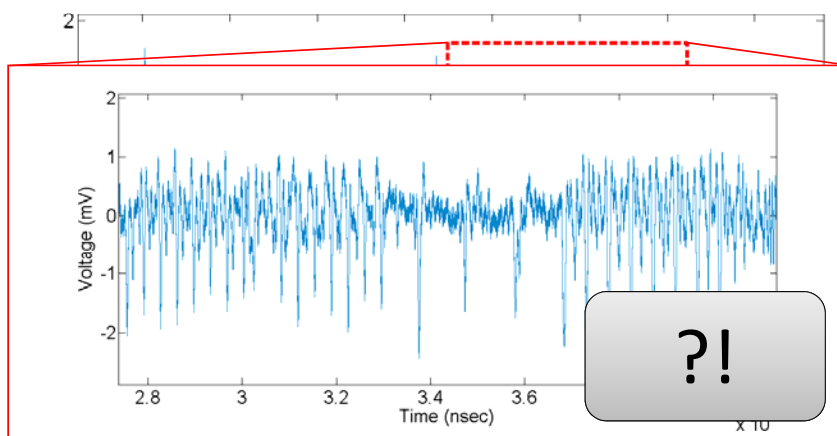
MIT CIS

### Digital Demodulation



MIT CIS

### Digital Demodulation

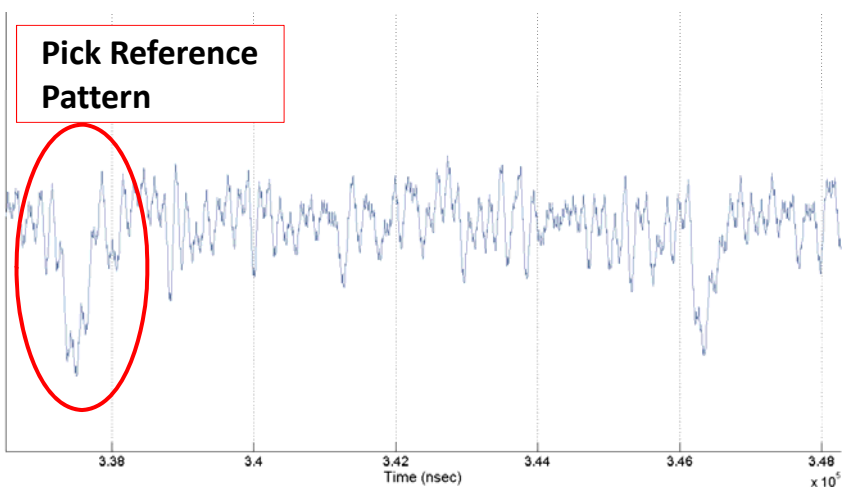


MIT CIS

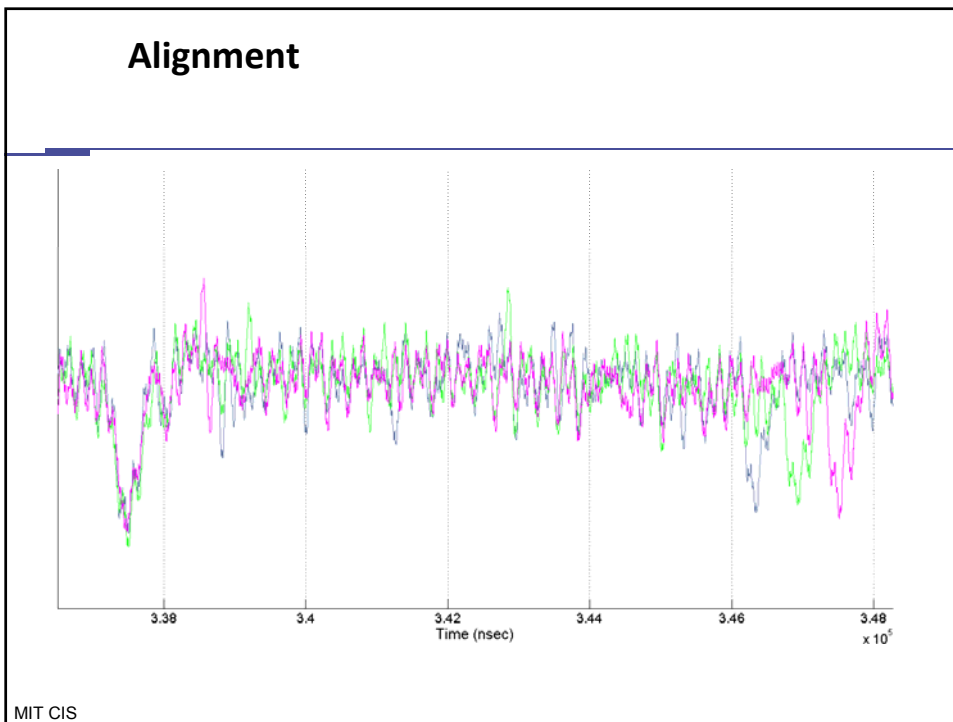
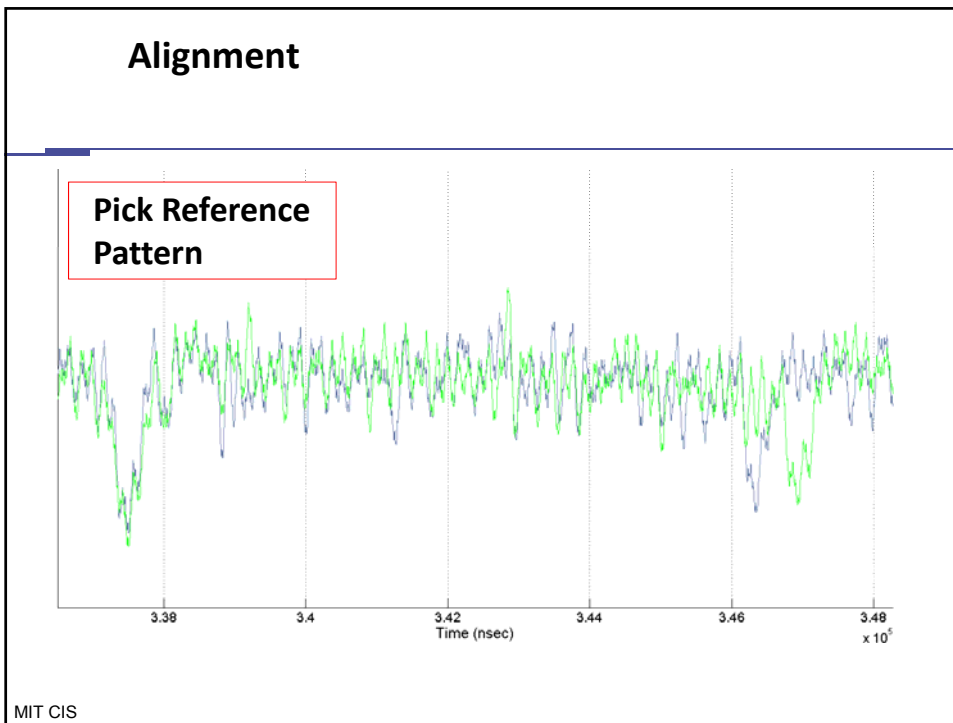
## Side Channel Analysis

### Step 4: Alignment

### Alignment

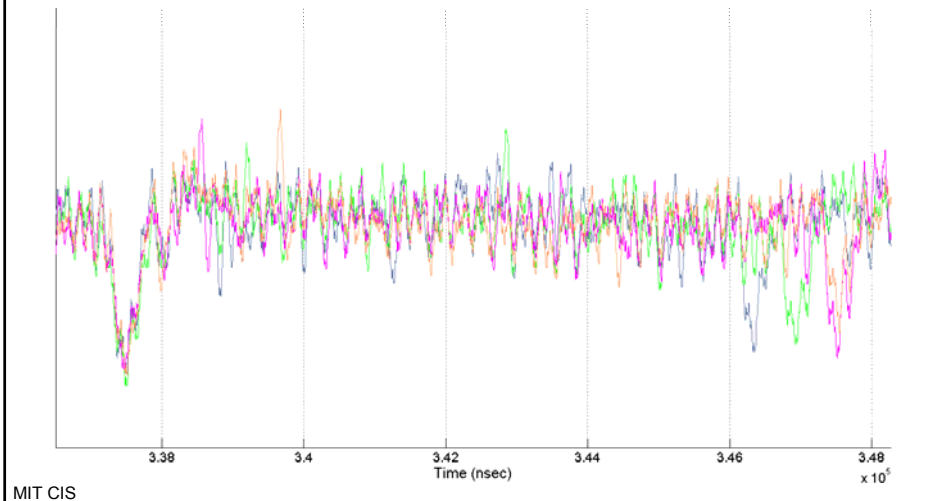


MIT CIS



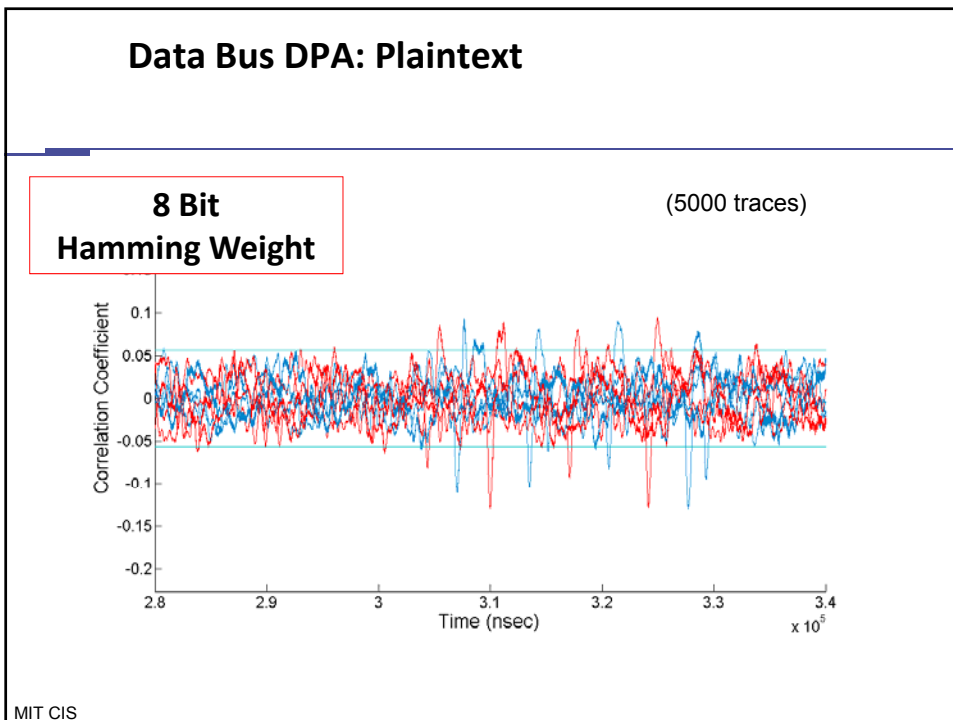
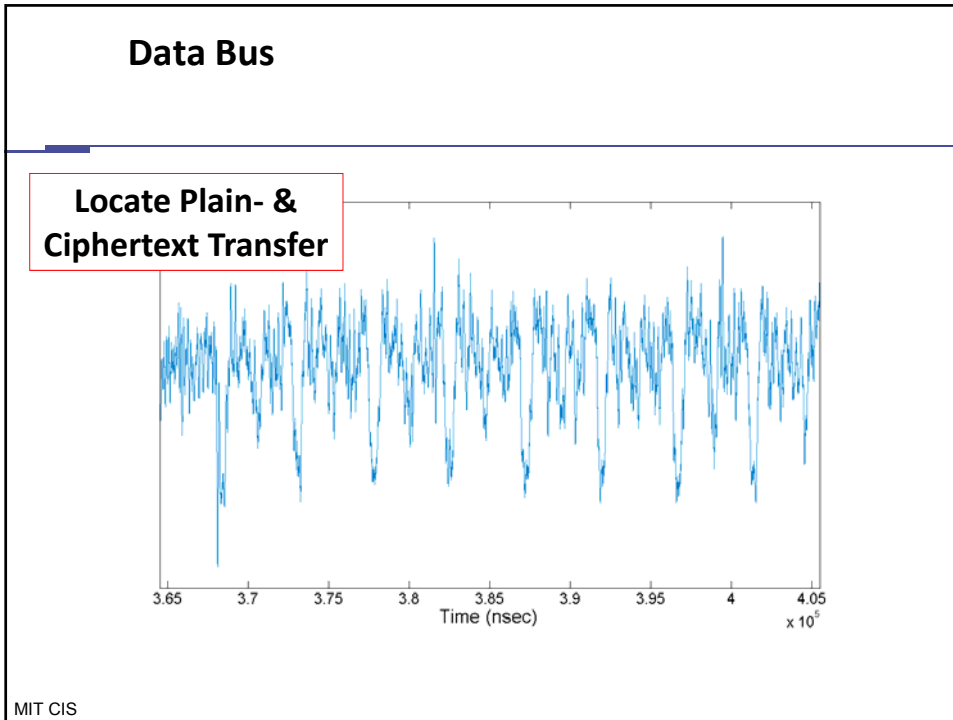
## Alignment

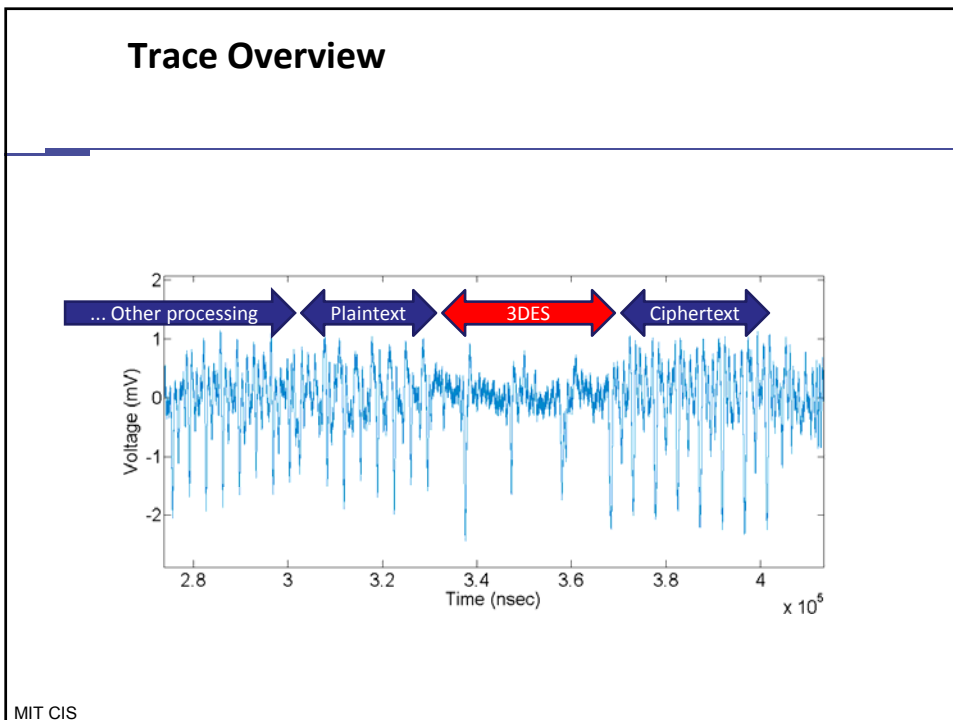
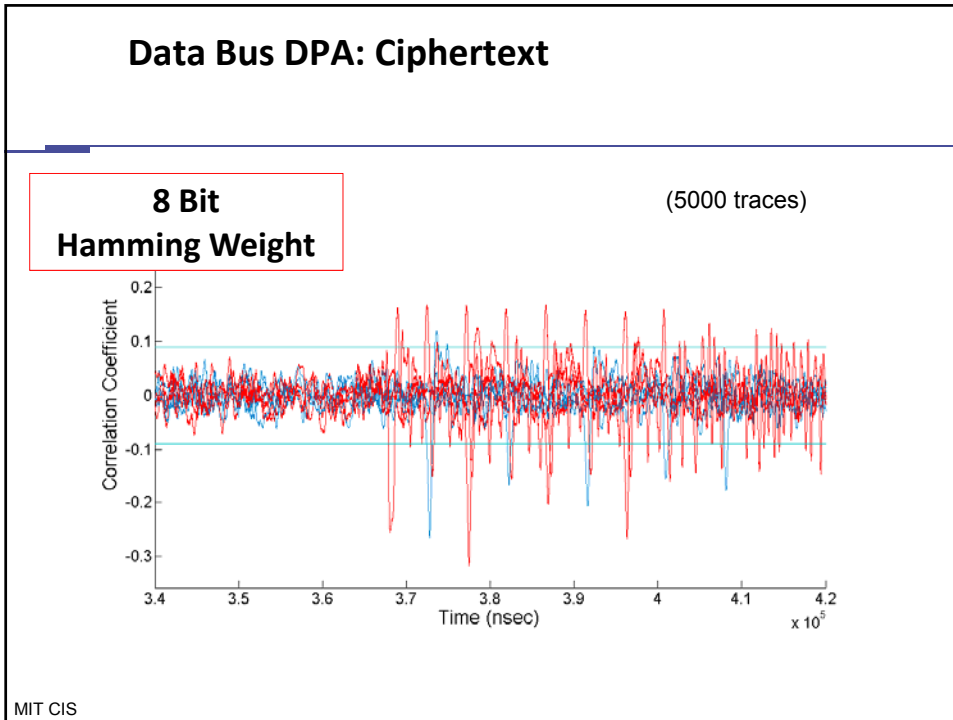
Varies for identical plaintexts → delay-variation as SCA countermeasure



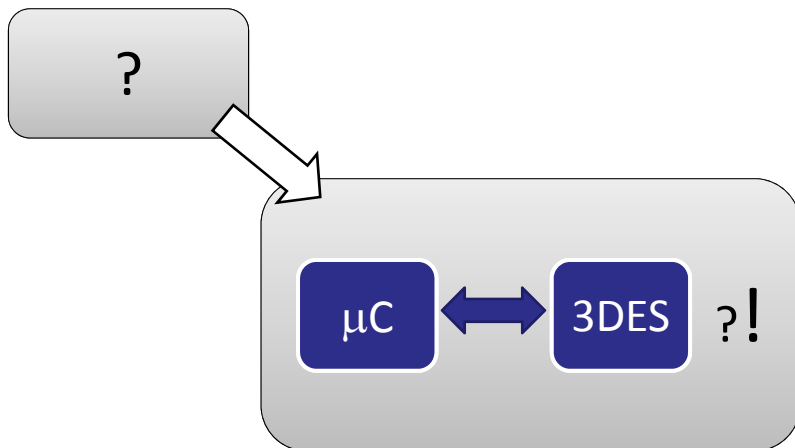
## Side Channel Analysis

**Step 5: Location of 3DES**  
(Profiling with fixed, known key)





## Working Assumption: 3DES Hardware Engine

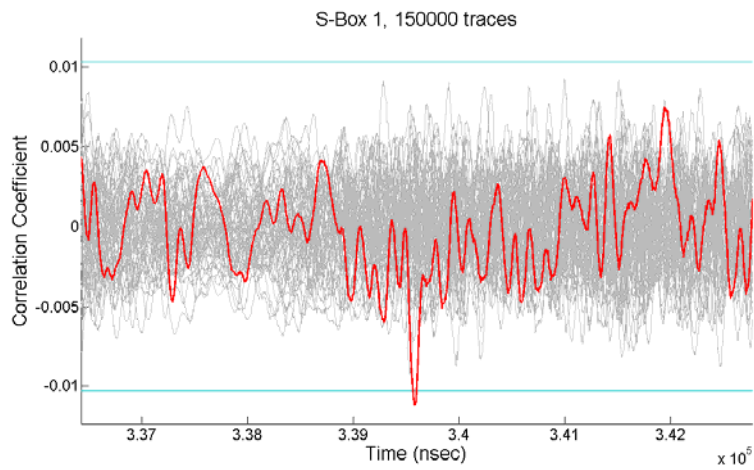


MIT CIS

## Side Channel Analysis

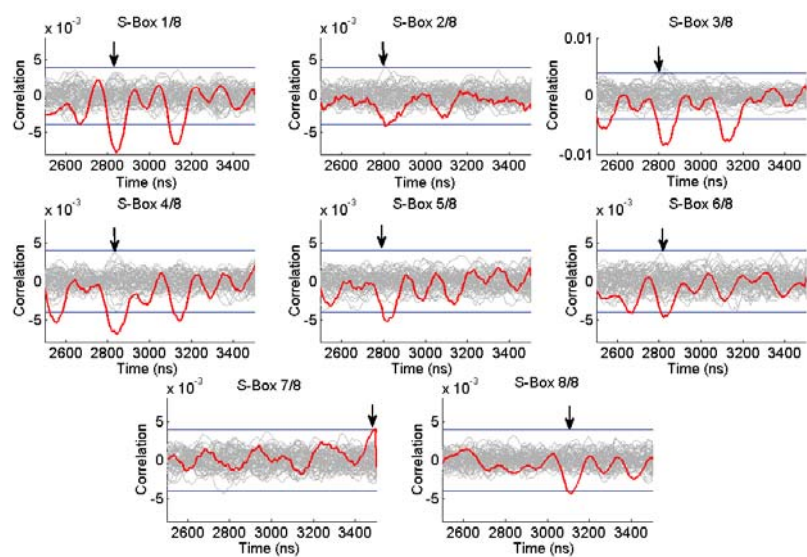
**Step 6: Attack**

### 3DES-Engine DPA



MIT CIS

### DES Full Key Recovery



MIT

## Summary

---

- card is advertised as *secure* alternative to Mifare
- full 3DES key revealed with  $\approx 100.000$  traces
- variants of attack can be much more powerful
- basic countermeasures are easy to overcome
- new generation of 3DES card will make SCA attacks more difficult
- ... but we would not rely on this
- Recommendation: **System design needed such that break of single crypto device can be contained (cf. magnetic-stripe credit cards)**

MIT CIS

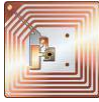
## Agenda

---

- Remote Access Control with KeeLoq
- Contactless Payments with Mifare Classic
- Contactless Smartcards with 3DES
- **Auxiliary Stuff**

MIT CIS

## Related Workshops



**SECSI – Secure Component and Systems Identification**  
April 2010, Cologne, Germany

**CHES – Cryptographic Hardware and Embedded Systems**  
co-located with Crypto!  
August 2010, UCSB

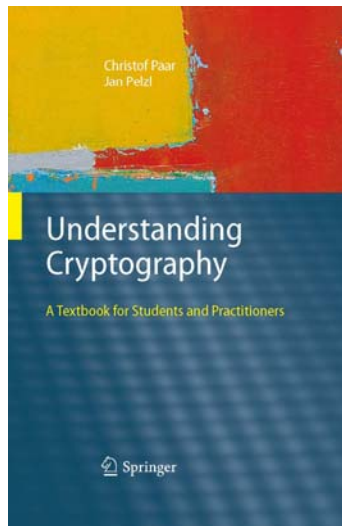


**escar – Embedded Security in Cars**  
November 2010, Bremen, Germany

## Post-Doc Position in Embedded Security Group @ U Bochum

- Work on theoretical and/or practical aspects of physical attacks
- Great working atmosphere (or so they say)
- Please contact Christof Paar, [cpaar@crypto.rub.de](mailto:cpaar@crypto.rub.de)

... and yet another textbook on cryptography



- Hopefully helpful for people without PhD's in mathematics
- Quite comprehensive
- [www.crypto-textbook.com](http://www.crypto-textbook.com)

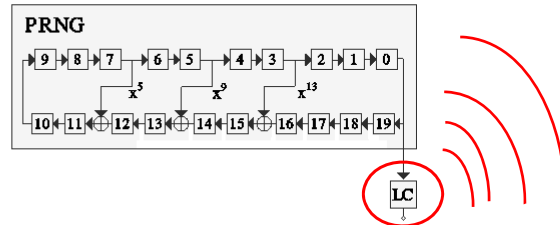
MIT CIS

Thanks for your attention!

Christof Paar  
[www.crypto.rub.de](http://www.crypto.rub.de)



## Spread spectrum based watermarks



Two Components that are added to the IP core:

1. A PRNG that generates a pseudo-random bit sequence
2. A **Leakage Circuit (LC)** that is attached to the PRNG and that leaks out the bitstream

MIT CIS

## Detecting a spread spectrum based watermark

1. Measure a single long power trace of the targeted device
2. From this power trace derive exactly one power-value  $p_i$  for each of the  $n$  measured clock cycles. (e.g. by averaging the points of one clock cycle)
3. Compute the expected watermarking bit stream  $B=b_1, \dots, b_n$
4. Generate different Hypotheses  $H_i$  by shifting the bit stream  $B$ :
 
$$H_1=b_1, \dots, b_n$$

$$H_2=b_2, \dots, b_n, b_1$$
 ...
5. Correlate the Hypotheses  $H_i$  with the power-values  $P=p_1, \dots, p_n$
6. If the un-shifted bit stream ( $H_1$ ) generates a significant correlation peak, the watermark is embedded in the targeted device.

MIT CIS

## Practical results

**Implemented:** A 1<sup>st</sup> order DPA resistant AES implementation with an embedded spread-spectrum watermark.

**Device:** Xilinx Virtex-2 PRO  
XC2VP7-5 FPGA @ 24MHz



MIT CIS

## Practical results

**The used PRNG:**

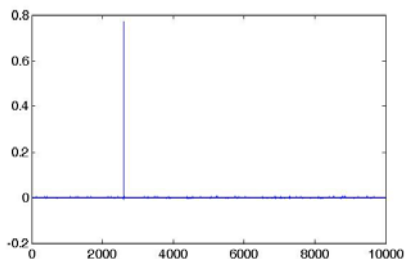
A 32-bit LFSR with  $X_{32} + X_{22} + X_2 + X_1$  and a fixed initial state.

**The used Leakage Circuit:**

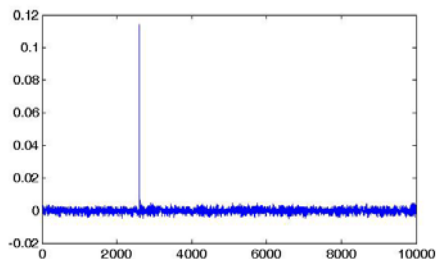
- 16-bit Shift-Register
- initialized with 0xAAAA
- shifted only if output of the PRNG is „1“

MIT CIS

## Measurements



Correlation for 500.000 clock cycles while the AES implementation was idle.



Correlation for 500.000 clock cycles while the AES implementation was constantly running.

MIT CIS

## Auxiliary Stuff

MIT CIS

## Conclusions

- Experience from real-world attacks are very valuable for the scientific community
- Real-world impact of (physical) attacks sometimes hard to assess
- Evolution of physical attacks are an interesting (and scary) phenomenon
- Is there a metric for measuring the hardness of physical attacks?

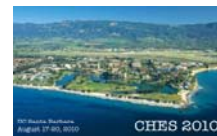
MIT CIS

## Related Workshops



**SECSI – Secure Component and Systems Identification**  
April 2010, Cologne, Germany

**CHES – Cryptographic Hardware and Embedded Systems**  
August 2010, UCSB



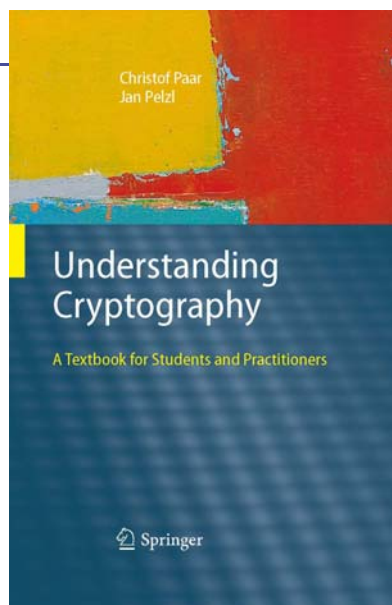
**escar – Embedded Security in Cars**  
November 2010

## Post-Doc Position in Embedded Security Group @ U Bochum

- Work on theoretical and/or practical aspects of physical attacks
- 1+ year position
- Full scientific position, great working atmosphere
- Please contact Christof Paar, [cpaar@crypto.rub.de](mailto:cpaar@crypto.rub.de)

MIT CIS

## ... and yet another textbook on Cryptography



- Hopefully helpful for people without PhD's in mathematics
- Quite comprehensive
- [www.crypto-textbook.com](http://www.crypto-textbook.com)

MIT CIS