Crypto Engineering: Some History and Some Case Studies

Invited Talk
CHES 2009
EPFL Lausanne, September 6-9, 2009

Christof Paar

Embedded Security Group EMSEC

Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany

www.crypto.rub.de

Overview

Horst-Görtz Institut
für IT Sicherheit

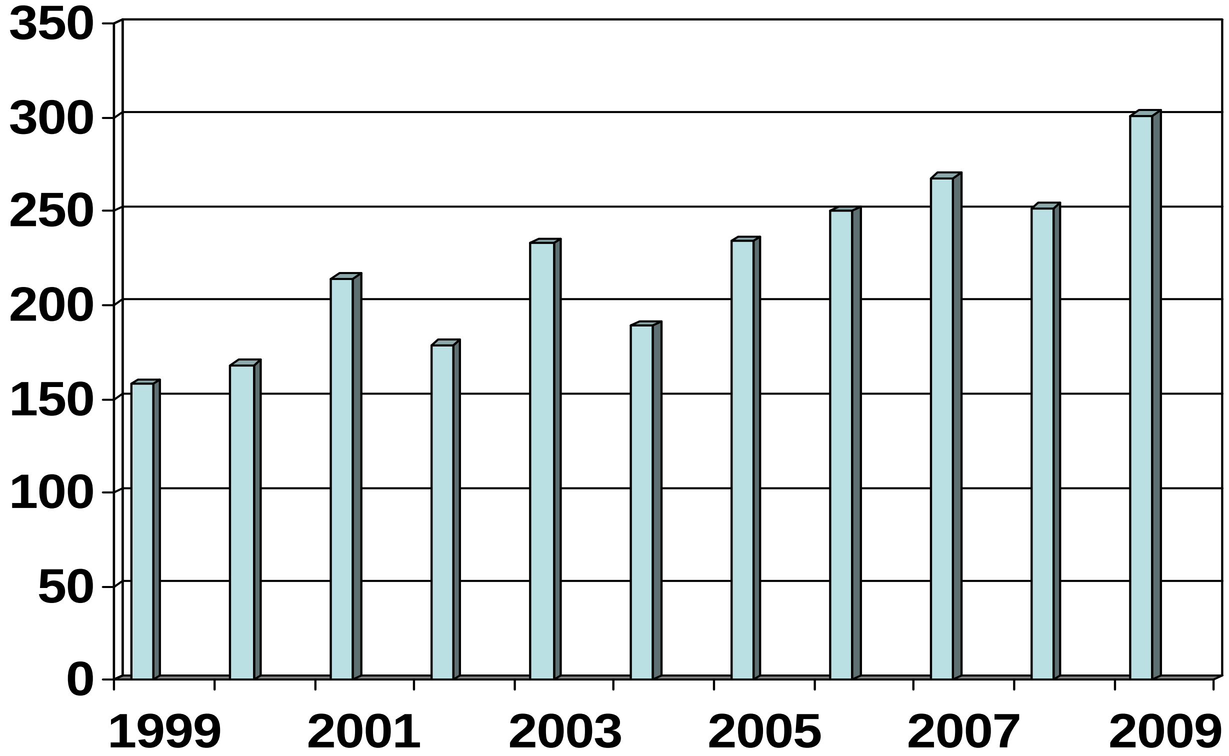
- How CHES Evolved
- Embedded Security Case Study 1: Batteries
- Embedded Security Case Study 2: Cars
- Embedded Security Case Study 3: Doors
- Some advertisements

Overview

Horst-Görtz Institut
für IT Sicherheit

- **How CHES Evolved**
- Embedded Security Case Study 1: Batteries
- Embedded Security Case Study 2: Cars
- Embedded Security Case Study 3: Doors
- Some advertisements

CHES registration over the years



A question I‘ve had for the last 10 years:

Why has CHES turned into such a popular event?

(especially while other crypto conferences have lost participants?)

My view on Crypto Engineering, ca. 1999

Crypto Engineering = Fast Asymmetric Implementations

Why has CHES become so popular?

Horst-Görtz Institut
für IT Sicherheit

A few possible reasons:

1. Side-Channel Attacks
2. AES
3. Cryptology Research Matured
4. Dot-Com Boom

Disclaimer: There is no proof of correctness for such sociological phenomena.

1. Side Channel Attacks

The CHES birth in 1999 coincided with the advent of SCA

- Bellcore attack (fault injection) in 1996
- SPA, DPA in 1998

Consequences of the attack

1. The smart card industry was under shell shock
2. People discovered a great new area to generate research papers

Even though not intented by the CHES founders, the scientific community picked CHES as its favorite publication outlet for side-channel papers.

I had to extend my model…

Crypto Engineering = Fast Asymmetric Implementations

+

Secure Implementations

2. AES

AES process began in 1997

- ca. 1999 implementers became interested in block ciphers
- much research dealing with fast + small AES candidates in hardware (e.g., by Gaj et al.)
- … and in software (e.g., by Gladman)

$\Rightarrow$ CHES folks discovered symmetric ciphers as a research area

I had to extend my model again …

Crypto Engineering = Fast Asymmetric Implementations

\+

Secure Implementations

\+

Symmetric Implementations

3. Specialization of Crypto Community

1981 … 1993: Crypto communicty was well-served by :

CRYPTO + EUROCRYPT + ASIACRYPT (catch-all crypto conferences)

But then: 3 new conferences in 6 years:

- FSE (Fast Software Encryption) in 1993
- PKC (Public-Key Cryptography) in 1998
- CHES in 1999

$\Rightarrow$ 1990s was the decade where the crypto community matured

(Rem: Spezialization seems like a natural + healthy development)

4. Dot-Com Boom

Horst-Görtz Institut für IT Sicherheit

- Dot-Com bubble burst in earnest in 2001, i.e., after CHES 99 and 2000
- Increased awareness (and money) for security issues was available

5. Other factors

Again, the previous 4 reasons are without guarantee. There are several other (softer) factors possible:

- Great food
- Great locations
- Good organization
- Very active Program Chairs + Steering Committee

Conclusions:
Why has CHES become so popular?

1. Side-Channel Attacks
2. AES
3. Cryptology Research Matured
4. Dot-Com Boom
5. Great Food

Factors 1-4 were outside developments!

⇒ **The time was simply ripe for a conference like CHES! i.e., CHES was largely shaped by the environment and not vice versa**

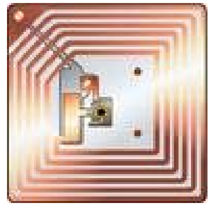
(cf. “Outliers” by Malcom Gladwell)

Overview

- How CHES Evolved
- **Embedded Security Case Study 1: Batteries**
- Embedded Security Case Study 2: Cars
- Embedded Security Case Study 3: Doors
- Some advertisements

Lightweight Cryptography

- “We need security with less than 2000 gates”
  Sanjay Sarma, AUTO-ID Labs, CHES 2002



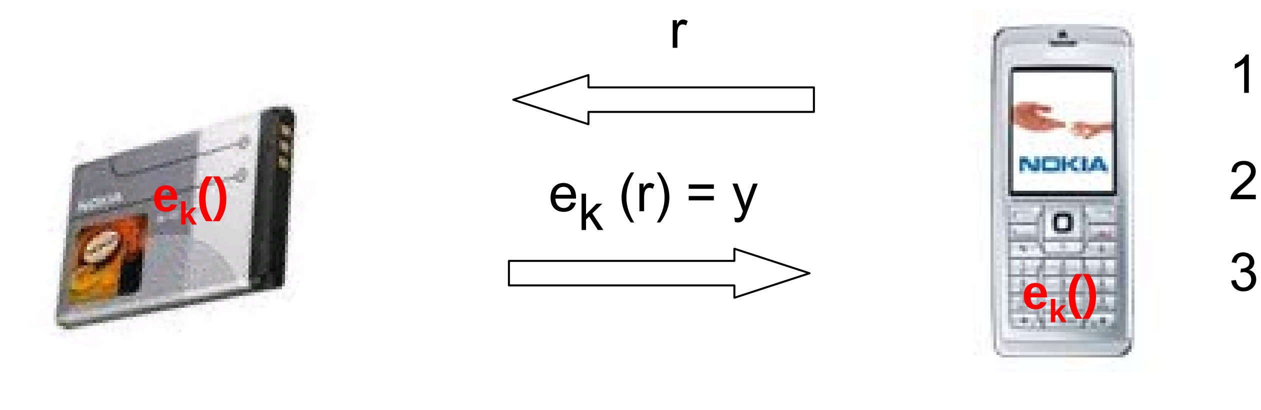
- $3 trillions annually due to product piracy* (> US budget ‘07)

*Source: www.bascap.com

⇒ Authentication & identification problem: can “easily” be fixed with standard crypto tools

Identification with Challenge-Response

Horst-Görtz Institut
für IT Sicherheit



1. random challenge r
2. encrypted response y
3. verification

   e_k (r) = y‘

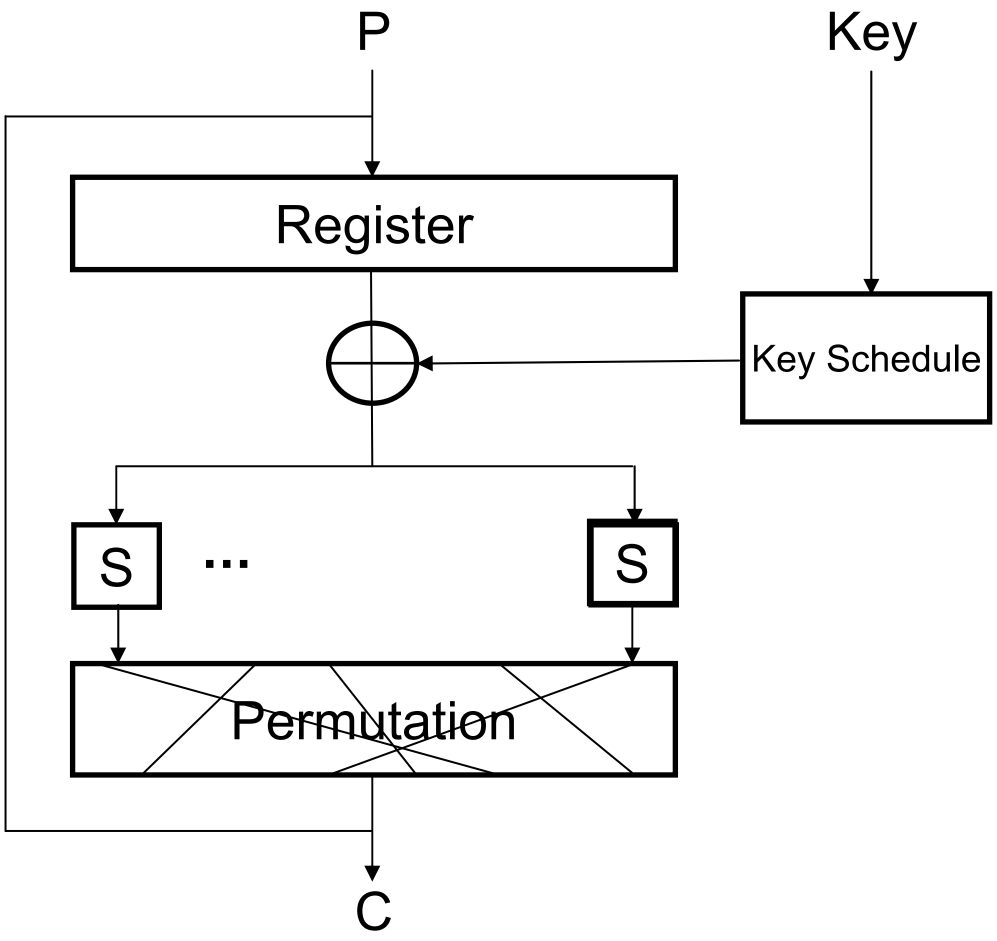
   y == y‘

Challenge: encryption function e() at extremely low cost (in hardware)

→ almost all symmetric ciphers optimized with SW in mind

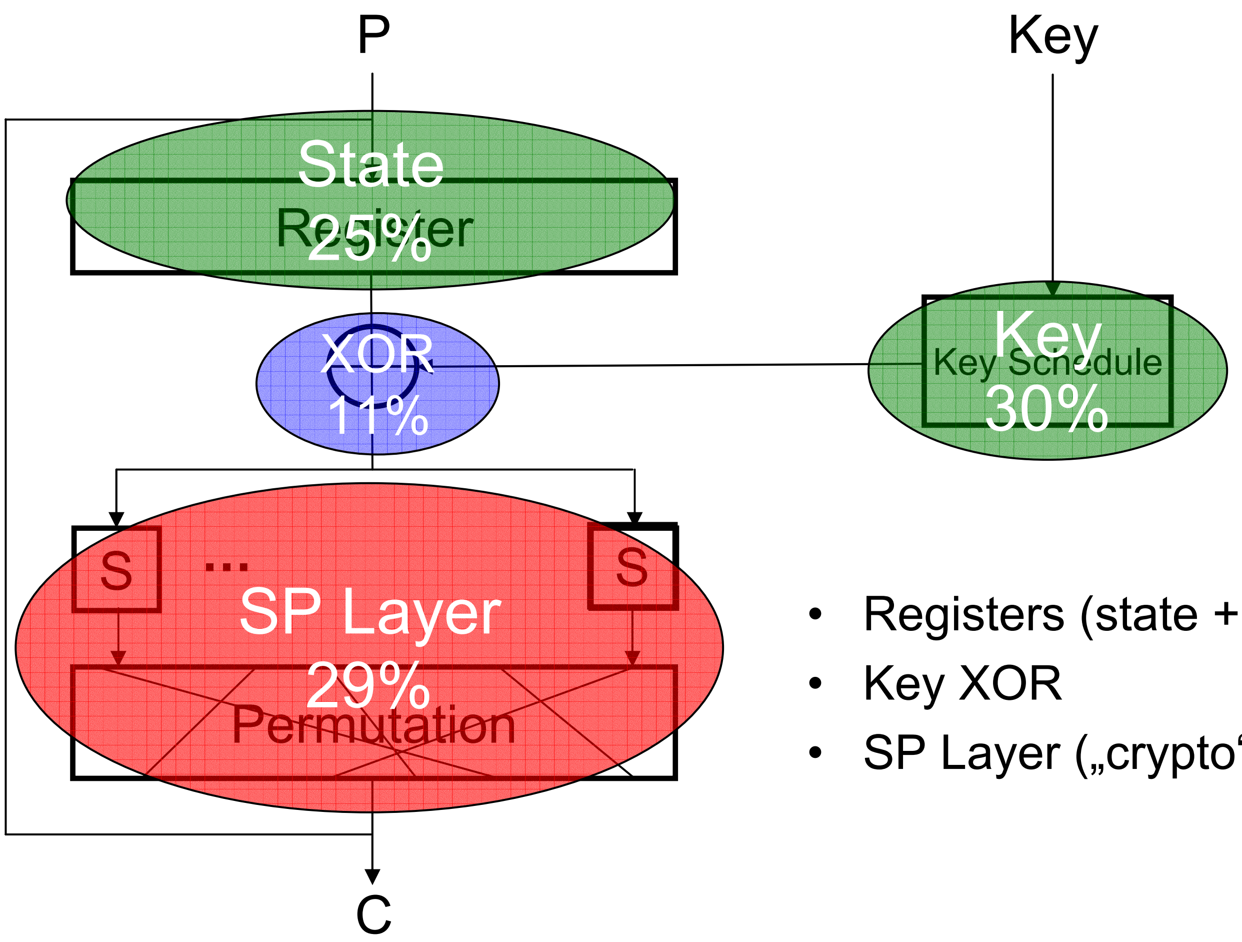
PRESENT – An agressively hardware optimized block cipher for RFID

- pure substitution-permutation network
- 64 bit block, 80/128 bit key
- 4-4 bit Sbox
- 31 round (32 clks)
- „provable secure“ against DC, LC
- joint work with Lars Knudsen, Matt Robshaw et al.
- no patents etc.



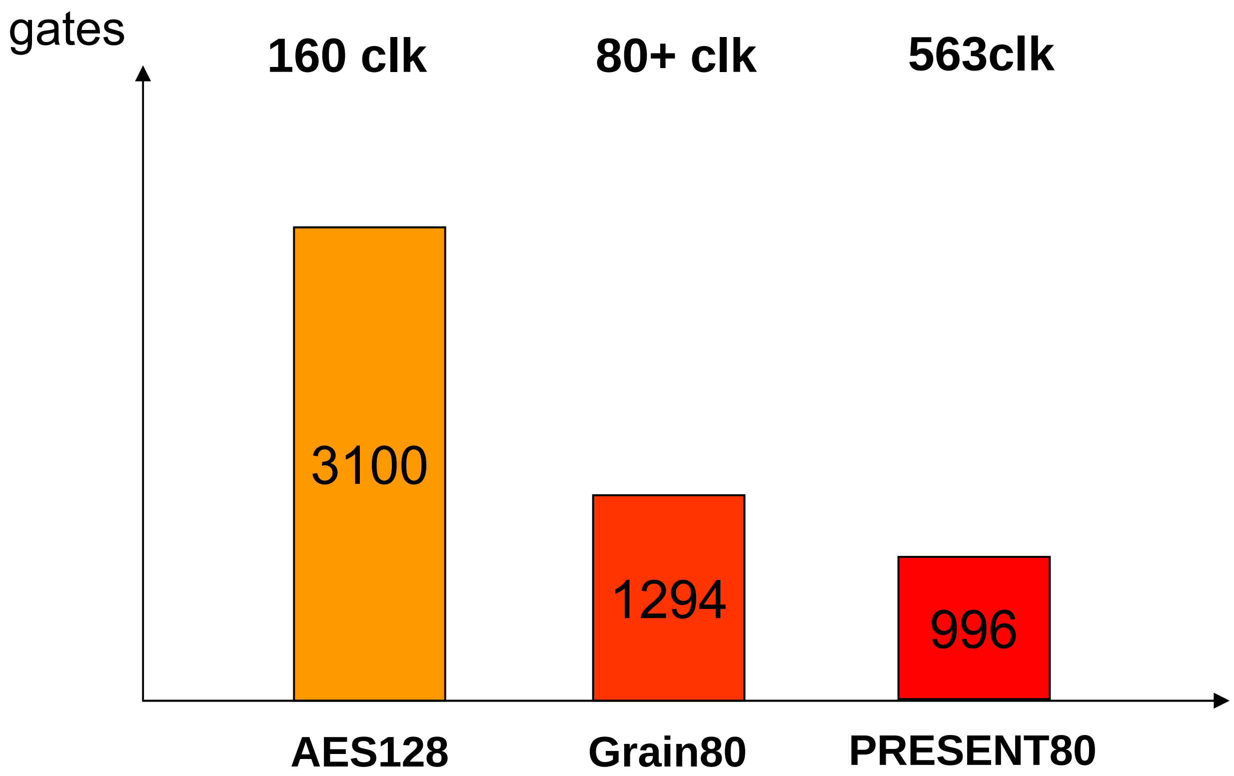
Resource use within lightweight ciphers

Round-parallel implementation of PRESENT (1570ge)



- Registers (state + key) 55%
- Key XOR 11%
- SP Layer („crypto“) 29%

Gate count of small ciphers



- Theoretical limit ≈ 900 gates (storing of 64 state + 80 key)

Overview

- How CHES Evolved
- Embedded Security Case Study 1: Batteries
- **Embedded Security Case Study 2: Cars**
- Embedded Security Case Study 3: Doors
- Some advertisements

Crypto in Cars

Horst-Görtz Institut
für IT Sicherheit

- USA: 42,000+ car fatalities per year (IIHS, 2002)
- 3.2m injuries (2000)
- est.: 90% driver errors

Video courtesy of Ken Labertaux, Toyota Research

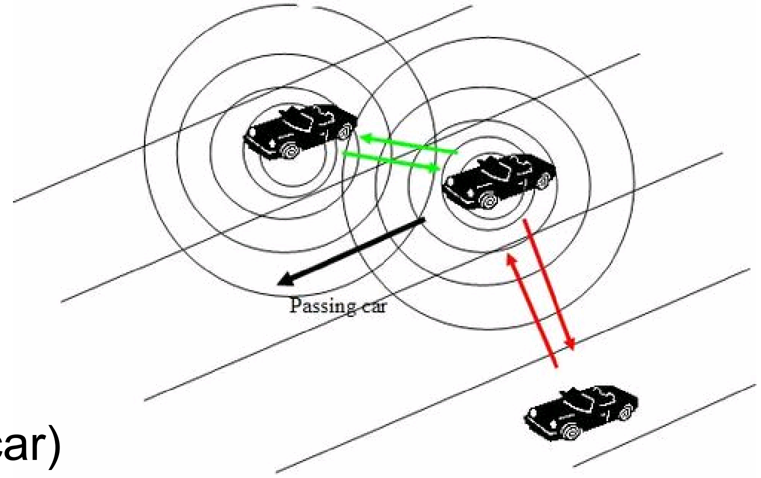
→ Mechanical saftey (safety belt, air bag, ABS): great success but limits have been reached

→ *Electronic driver assistance* will be key tool

VANET – Vehicular Ad-Hoc Networks

Broadcast position & direction information:

1. greatly improve safety
2. improve traffic management



Network characteristics

- small messages (≈ 100 Bytes)
- medium frequency (≈ 10 messages/sec per car)
- very ad-hoc (short lived, high dynamics)
- high number of incoming messages (> 1000msg/sec per car)
- IEEE P1609/DSRC standard

But messages must be authenticated!
(IEEE P1363: ECDSA)

Elliptic Curve Primitive

- Given a Point P on an elliptic curve E over GF(p):

$$E:\ y^2=x^3+ax+b \bmod p$$

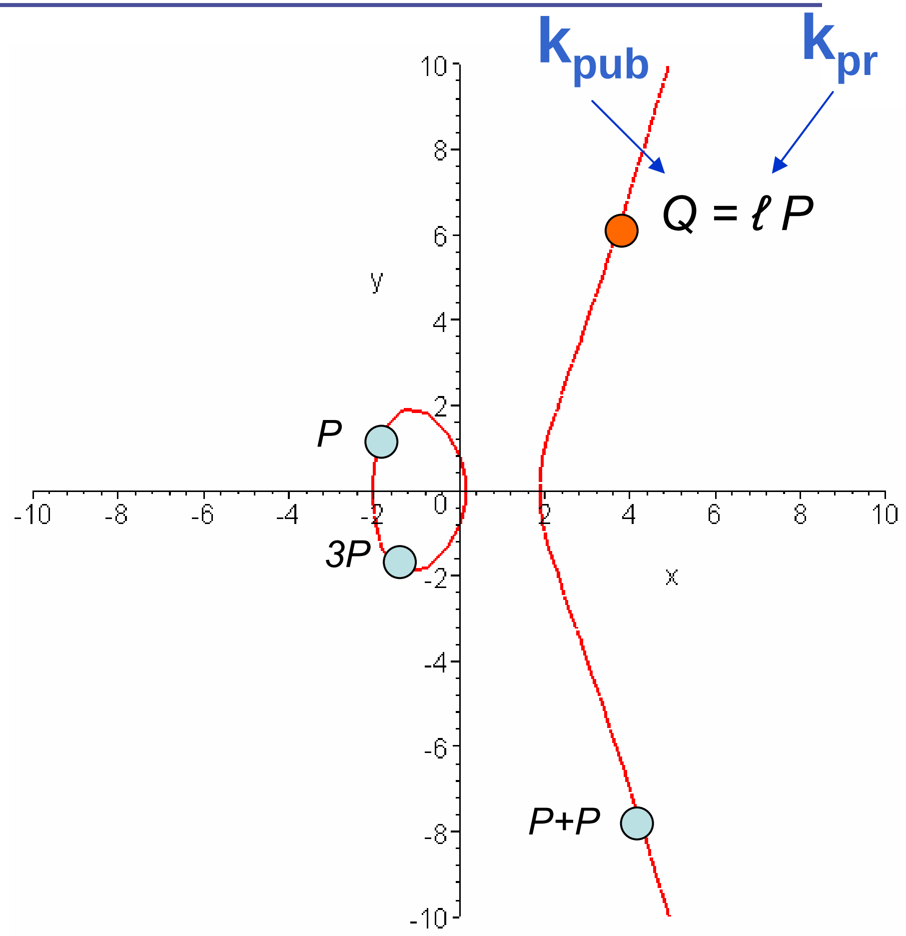
- Public key Q is multiple of base point P

group operation

$$Q = P+P+\ \dots\ +P = \ell P$$

- EC discrete logarithm problem:

$$\ell = dlog_P(Q)$$



Point Addition on EC

Jacobian Coordinates over GF(p)

Horst-Görtz Institut
für IT Sicherheit

- **Point Addition** R = P + S
- Input $P = (X_1, Y_1, Z_1)$; $S = (X_2, Y_2, Z_2)$
- Output $R = (X_3, Y_3, Z_3)$

$A = X_1 Z_2^2 \bmod p$

$B = X_2 Z_1^2 \bmod p$

$C = Y_1 Z_2^3 \bmod p$

$D = Y_2 Z_1^3 \bmod p$

$E = B - A \bmod p$

$F = D - C \bmod p$

$\boldsymbol{X_3} = -E^3 - 2AE^2 + F^2$ $\boldsymbol{Y_3} = -CE^3 + F(AE^2 - X_3)$ $\boldsymbol{Z_3} = Z_1 Z_2 E$

$\boxed{1 \text{ Point Add} = 14\ MUL_{256bit} = 3584\ MUL_{16bit}}$

Real-Time Signature Engine for VANETs

Horst-Görtz Institut
für IT Sicherheit

Requirements

- 256bit ECC Engine (long-term security)
- 1000 sign./sec → 1,000,000,000 Mul_{16} /sec
- acceptable cost & power

VANET Signature Engine

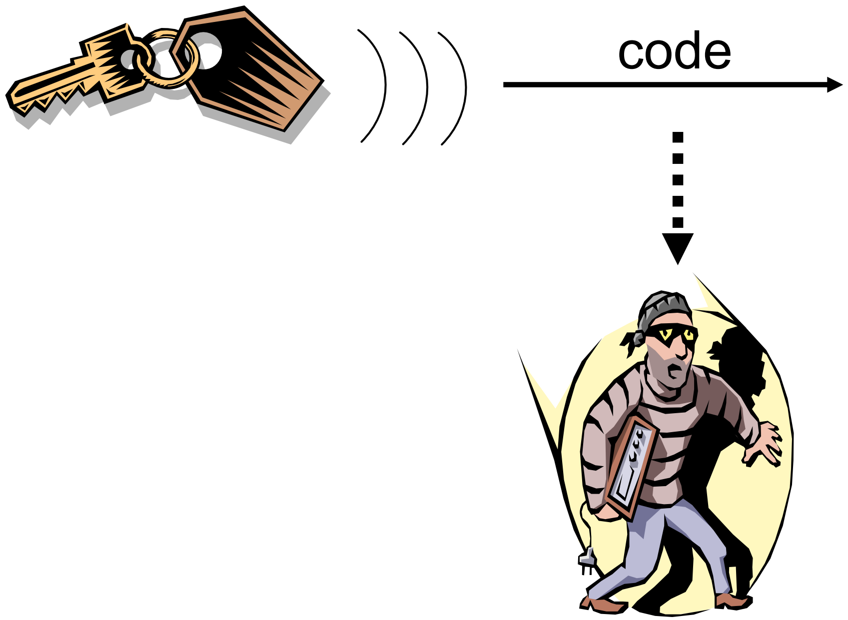
- **1 ECC VANET engine: > 1500 signatures/sec**
- 1 Mul_{256} requires 63 cycles@500MHz
- relies on cheap off-the-shelf FPGA w/ DSP-kernels
- (several 10,000 sign/sec possible with expensive off-the-shelf FPGA)

Overview

- How CHES Evolved
- Embedded Security Case Study 1: Batteries
- Embedded Security Case Study 2: Cars
- **Embedded Security Case Study 3: Doors**
- Some advertisements

Case Study Access Control

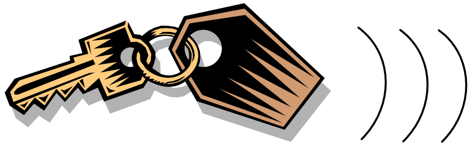
- Simple access controls: fixed code (“password”)



- eavesdropper duplicates key (cloning)
- but the industry learned…

Case Study Access Control

- advanced theft control: rolling code



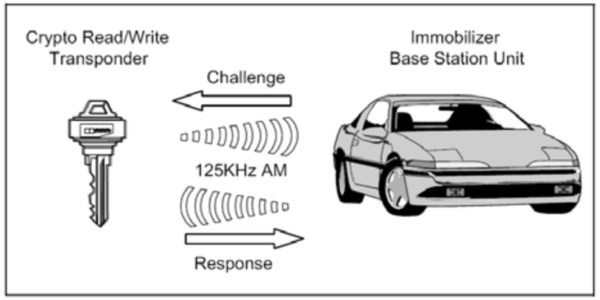
code = $e_k(n_i)$

$e_k()$ is often a block cipher

- rolling code (or hopping code)
- code = $e_k(n)$
- code = $e_k(n+1)$
- code = $e_k(n+2)$
- ….

Popular Rolling Code Cipher: KeeLoq

HCS410 IMMOBILIZER TRANSPONDER

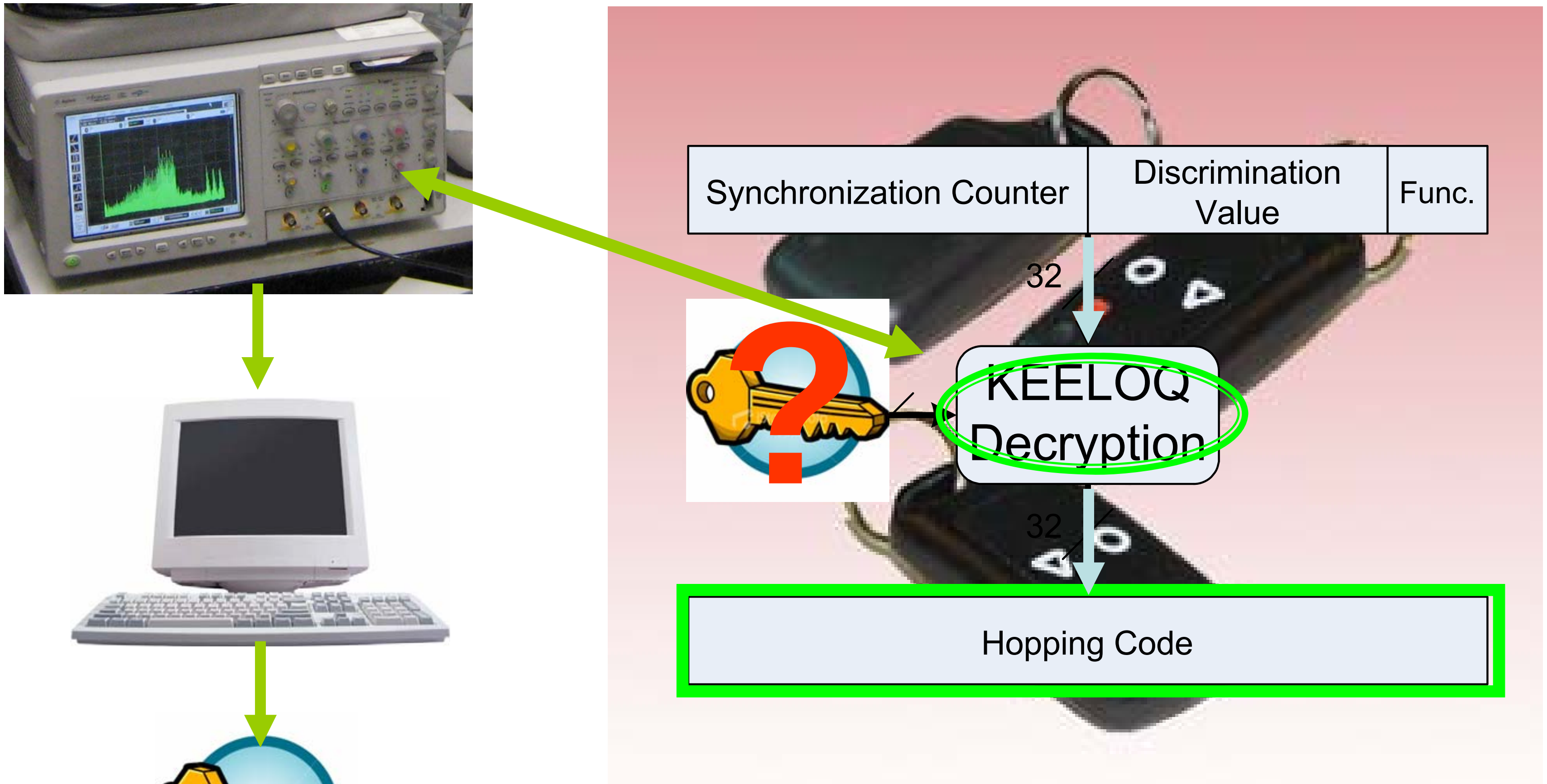


- Garage door access, car access, user authentication, …
- KeeLoq chip embedded in passive or active RFID transponder („car key“)
- Wikipedia (?):
  Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Jaguar, ...

Q: How secure is KeeLoq?

- best mathematical attack: 65,000 encryptions + plaintext
- works only for certain (weak) key derivations
- but: also „secure“ against physical attacks?

Side Channel Analysis



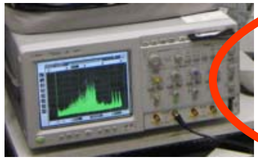
secret key of remote control (HCS XXX Chip) !

Performing the Side-Channel Attack

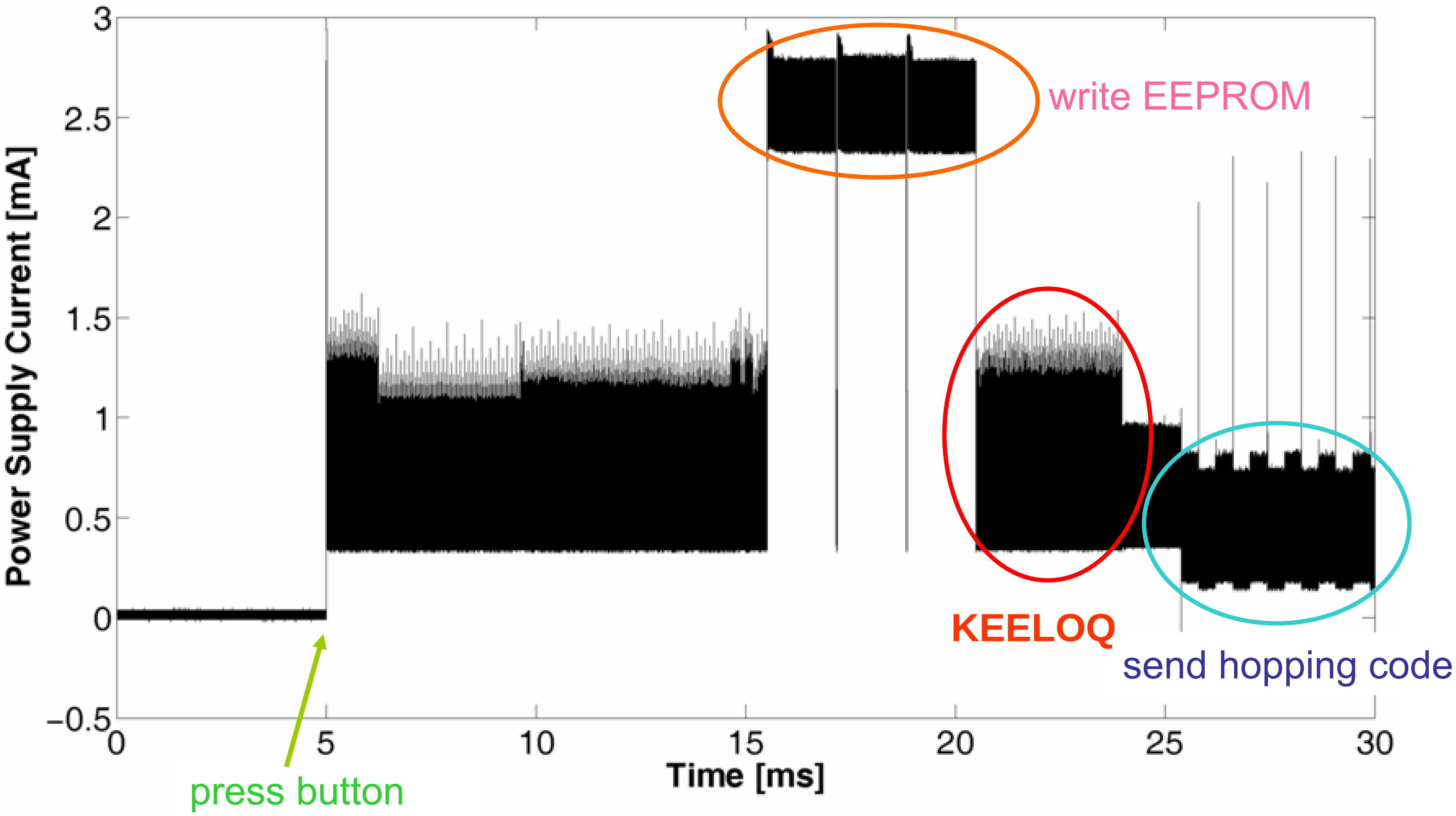
Horst-Görtz Institut für IT Sicherheit

KeeLoq CODE HOPPING

Analyze cipher	• Find a suited predictable intermediate value in the cipher
Measurements	• Measure the power consumption
Post Processing	• Post-process acquired data
Key Recovery	• Perform the attack to recover the key



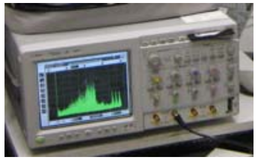
Side-Channel Attack Measurements of KeeLoq



Performing the Side-Channel Attack

Analyze cipher

- Find a suited predictable intermediate value in the cipher



Measurements

- Perform power measurements

Post Processing

- Post-process acquired data

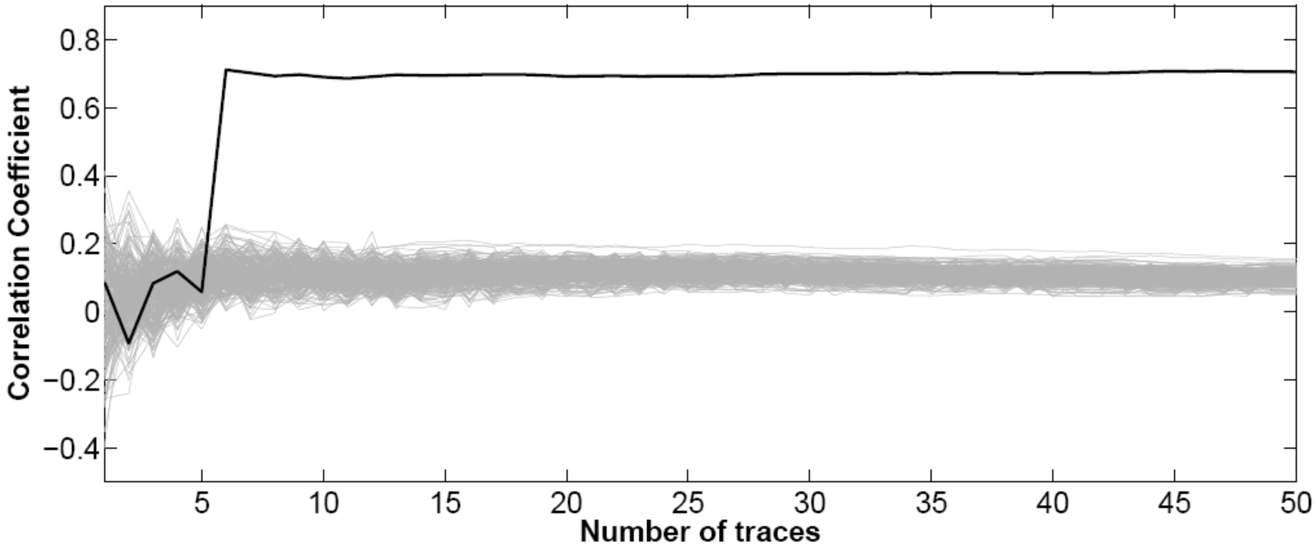
Key Recovery

- Perform the attack to recover the key

Side Channel Attack on transmitters

KeeLoq implemented in hardware

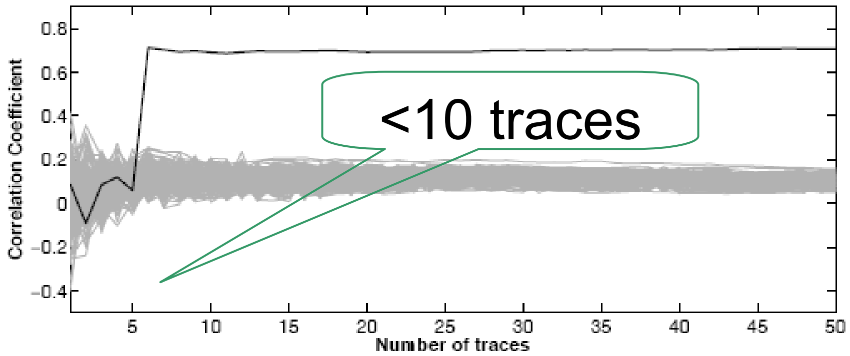
Total attack time (for known device family):
5-30 traces, ≈ minutes



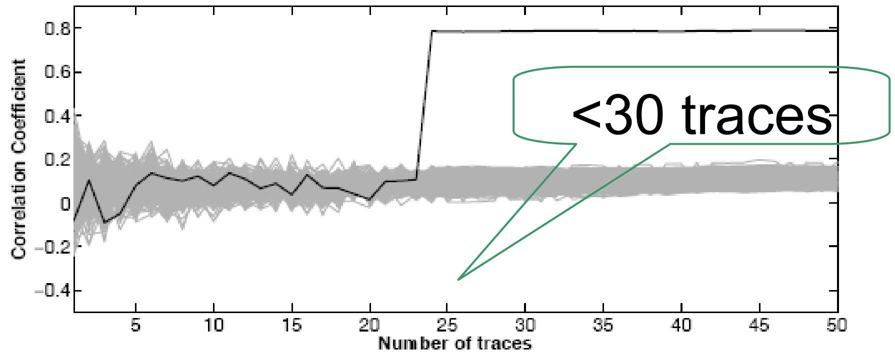
Convergence of correlation coefficient

Remark: low cost equipment suffices (< $1000)

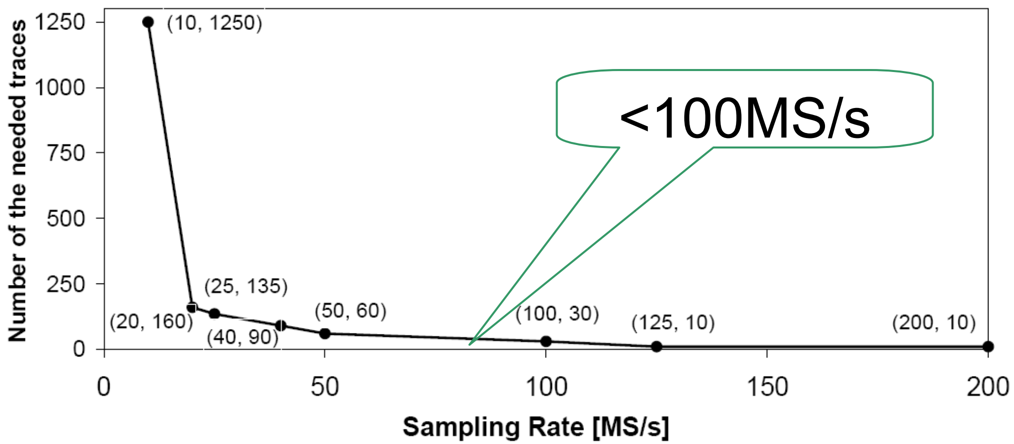
Comparison of Packages & Sample Rates



(a) DIP



(b) SOIC



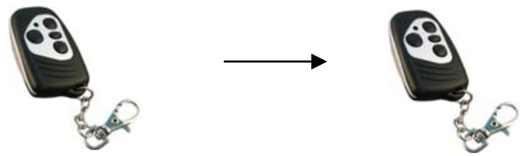
No expensive equipment needed !

Rem: SCA on receivers (software) requires several 1000 traces

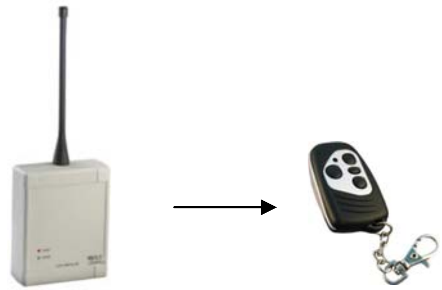
So what can we do now?

If we have access to a remote

Recover device key and clone the device



If we have access to a receiver

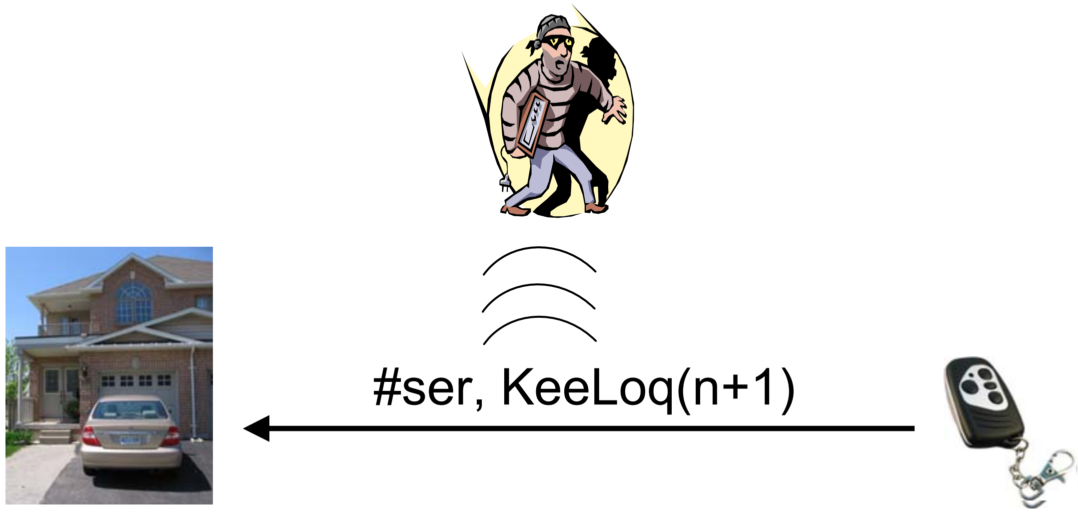


Recover manufacturer key and generate new remotes

So what can we do now (2) ?

After extracting of manufacturing key:

Remotely eavesdrop on 1-2 communications & clone key!



- might require a few hours of computation
- 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 !

Overview

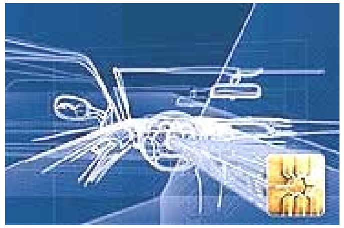
Horst-Görtz Institut
für IT Sicherheit

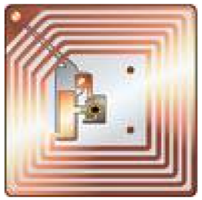
- How CHES Evolved
- Embedded Security Case Study 1: Batteries
- Embedded Security Case Study 2: Cars
- Embedded Security Case Study 3: Doors
- **Some advertisements**

Related Workshops

SHARCS – Special-purpose Hardware for Attacking Cryptographic Systems
September 2009, EPFL

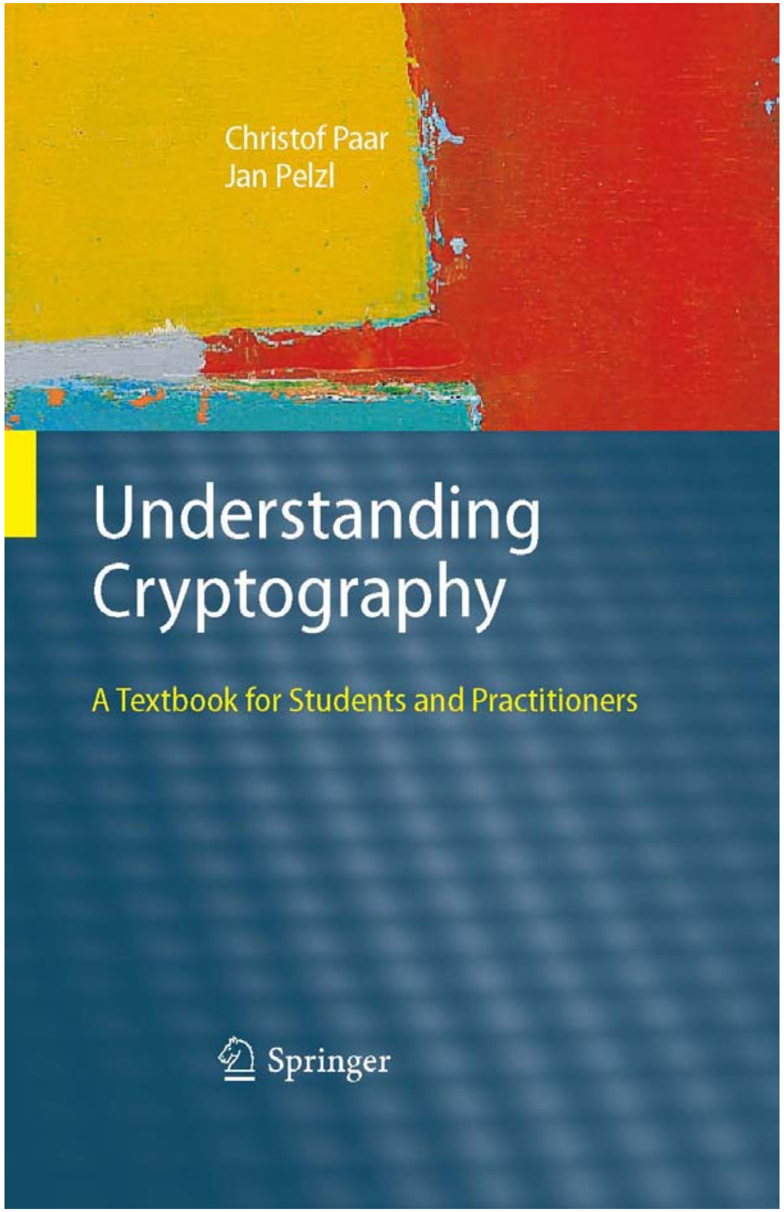
escar – Embedded Security in Cars
November 2009, Düsseldorf





SECSI – Secure Component and Systems Identification
2010

… and yet another textbook on Cryptography



- Hopefully helpful for people without PhD`s in mathematics
- Quite comprehensive
- www.crypto-textbook.com