On the Power of Power Analysis

A Complete Break of the Keyless Entry System *KeeLoq*

Timo Kasper

Embedded Security Group (Christof Paar)

Horst Görtz Institute for IT Security

Ruhr-University Bochum, Germany

ECC Workshop Utrecht, September 22-24, 2008

Agenda

Horst-Görtz Institut für IT Sicherheit

- Remote Keyless Entry (RKE) Systems
- KeeLoq Block Cipher
- Side-Channel Attacking KeeLoq
- Results and Implications

How do Keyless Entry Systems work?

Horst-Görtz Institut
für IT Sicherheit

early access controls: fixed code (“password”)

code

eavesdropper duplicates key (cloning)

but the industry learned…

Modern Keyless Entry Systems

Horst-Görtz Institut
für IT Sicherheit

advanced theft control: rolling code

$code = e_k(n_i)$

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

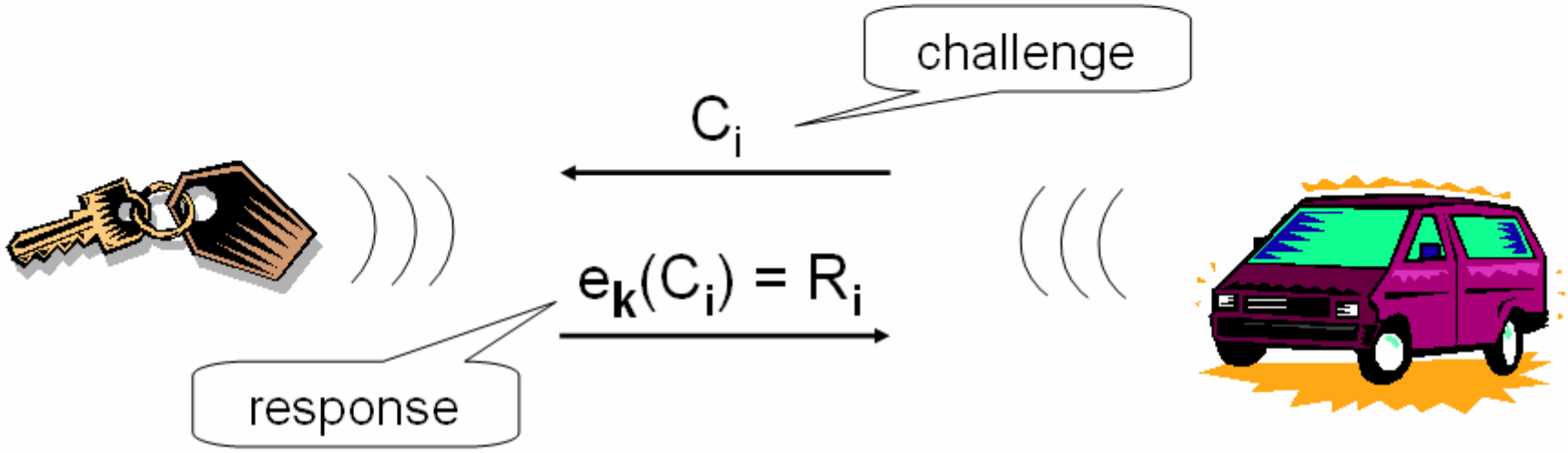
1. $code = e_k(n)$
2. $code = e_k(n+1)$
3. $code = e_k(n+2)$

....

$e_k()$ is often a block cipher

Alternative: Challenge-Response (aka IFF – Identify Friend or Foe)

Horst-Görtz Institut für IT Sicherheit



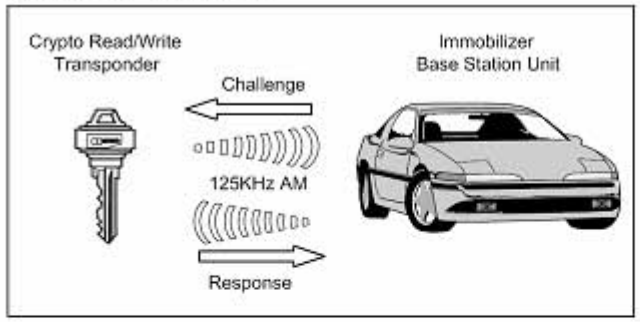
- again, $e_k()$ is often a block cipher
- also protects against replay attack
- € drawback: requires bidirectional devices on either side
- In most real-world car and building access control systems: rolling code

1. Computes: $R'_i = e_k(C_i)$
2. Verifies: $R'_i \stackrel{?}{=} R_i$

Popular Remote Keyless Entry Cipher: KeeLoq

Horst-Görtz Institut für IT Sicherheit

HCS410 IMMOBILIZER TRANSPONDER



KEELOQ CODE HOPPING

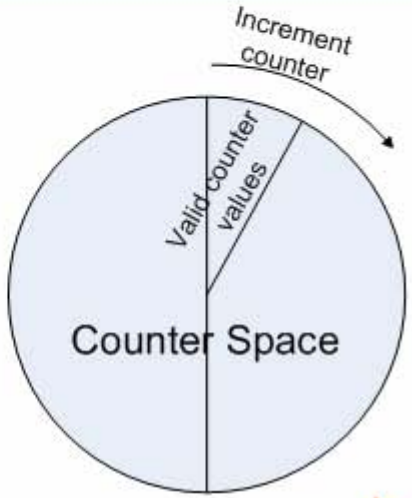
- KeeLoq can be used as rolling code or in a challenge-response protocol
- active remote control for access control
- KeeLoq chip embedded in passive RFID – transponder (e.g. for car immobilizer)
- Wikipedia (?):
  Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Jaguar, ...
- widely used for **garage doors** in US & Europe

Q: How secure is KeeLoq?

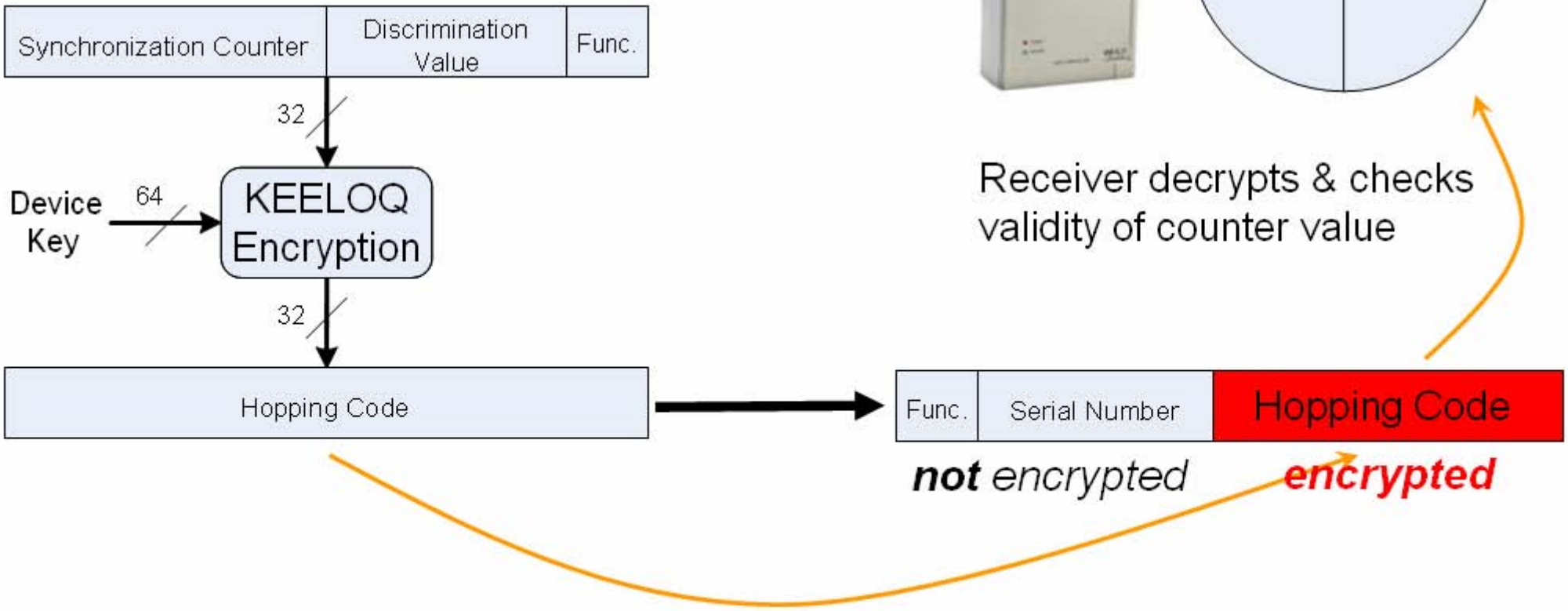
KeeLoq Rolling Code Scheme

Horst-Görtz Institut für IT Sicherheit

Counter: n+1



Receiver decrypts & checks validity of counter value



Key Management

OEM gets *Manufacturer Key* k_M assigned (burned in all its receivers)

1) Creation of new remote (in secure environment)

k_M

#ser

$k_{dev} = f(\#ser, k_M)$

Key derivation

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

#ser

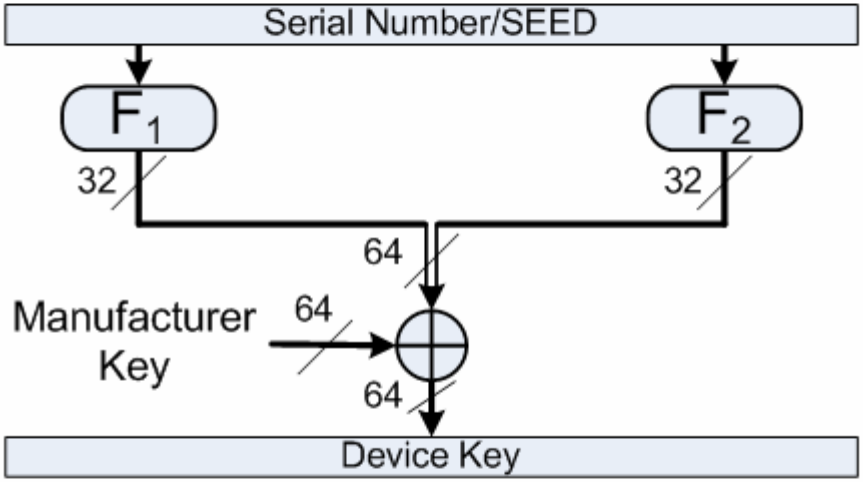
k_M

1. computes $k_{dev} = f(\#ser, k_M)$
2. stores $(\#ser, k_{dev})$

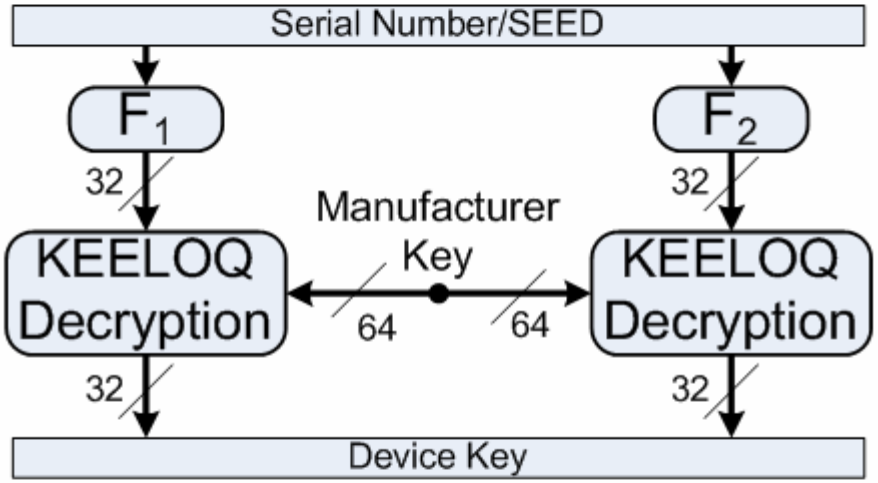
Key Derivation Schemes

Horst-Görtz Institut für IT Sicherheit

1. Weak Key Derivation (XOR)



2. Strong Key Derivation (KeeLoq)



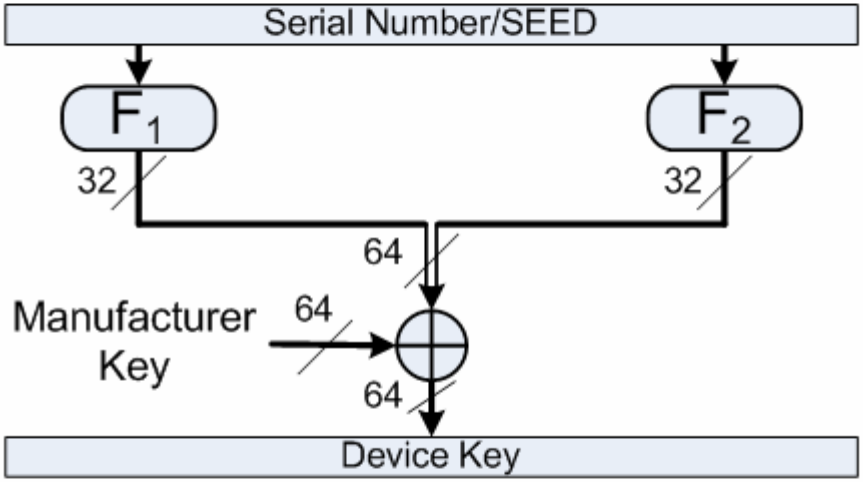
In either case, device key is derived from:

- Manufacturer key
- Serial number (known) or Random seed (32…60bits)

Key Derivation: Attacker's Assessment

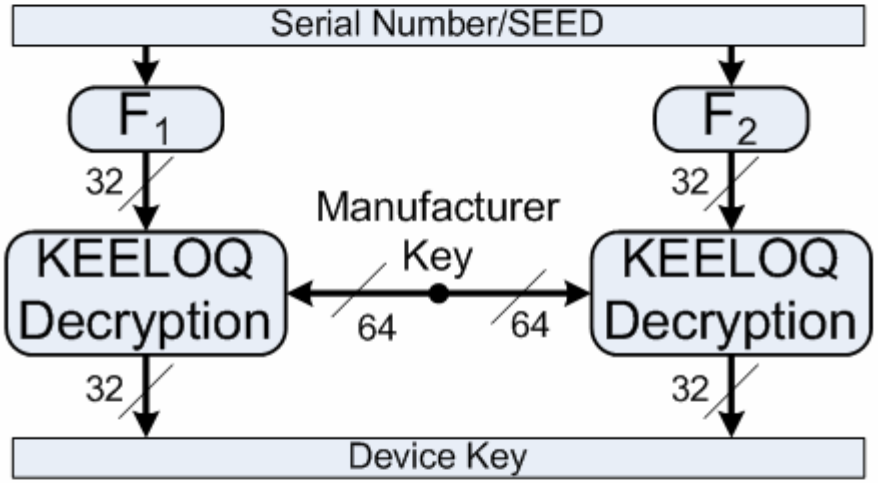
Horst-Görtz Institut für IT Sicherheit

1. Weak Key Derivation (XOR)



If we have the Device Key, getting the Manufacturer Key is trivial (and vice versa)

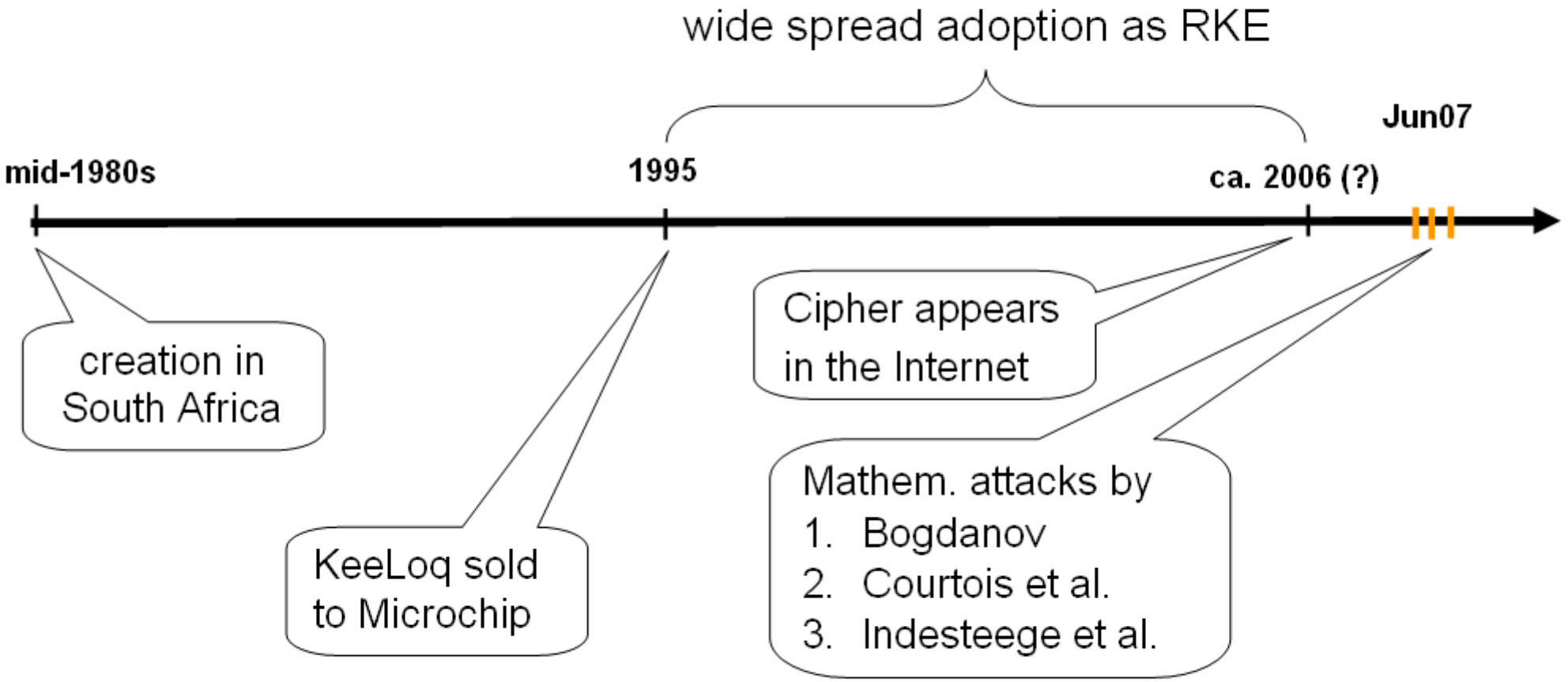
2. Strong Key Derivation (KeeLoq)



If we have the Device Key, we still have to break KeeLoq

Rise and Fall of KeeLoq

Horst-Görtz Institut
für IT Sicherheit



Mathematical Attacks: Recovery of Manufacturer Key

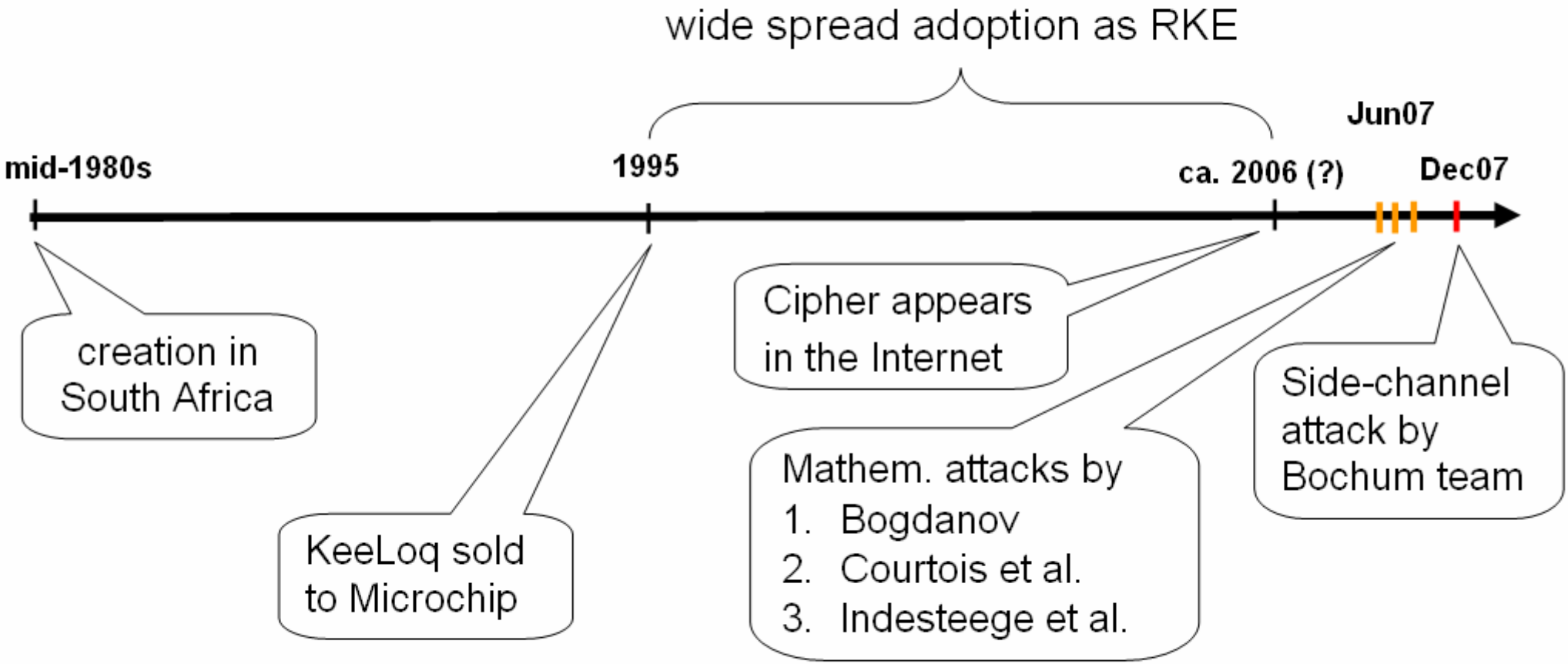
Horst-Görtz Institut für IT Sicherheit

	XOR Key Derivation	KeeLoq Key Derivation
Challenge-Response	Y	N
Rolling Code	N	N

- Mathematical attacks are cryptanalytically very impressive! Device Key is recovered from 2^{16} known plain/ciphertext pairs
- Problem: Rolling code mode does **not** provide plaintext!

- **Q: How dangerous are physical attacks?**

Rise and Fall of KeeLoq



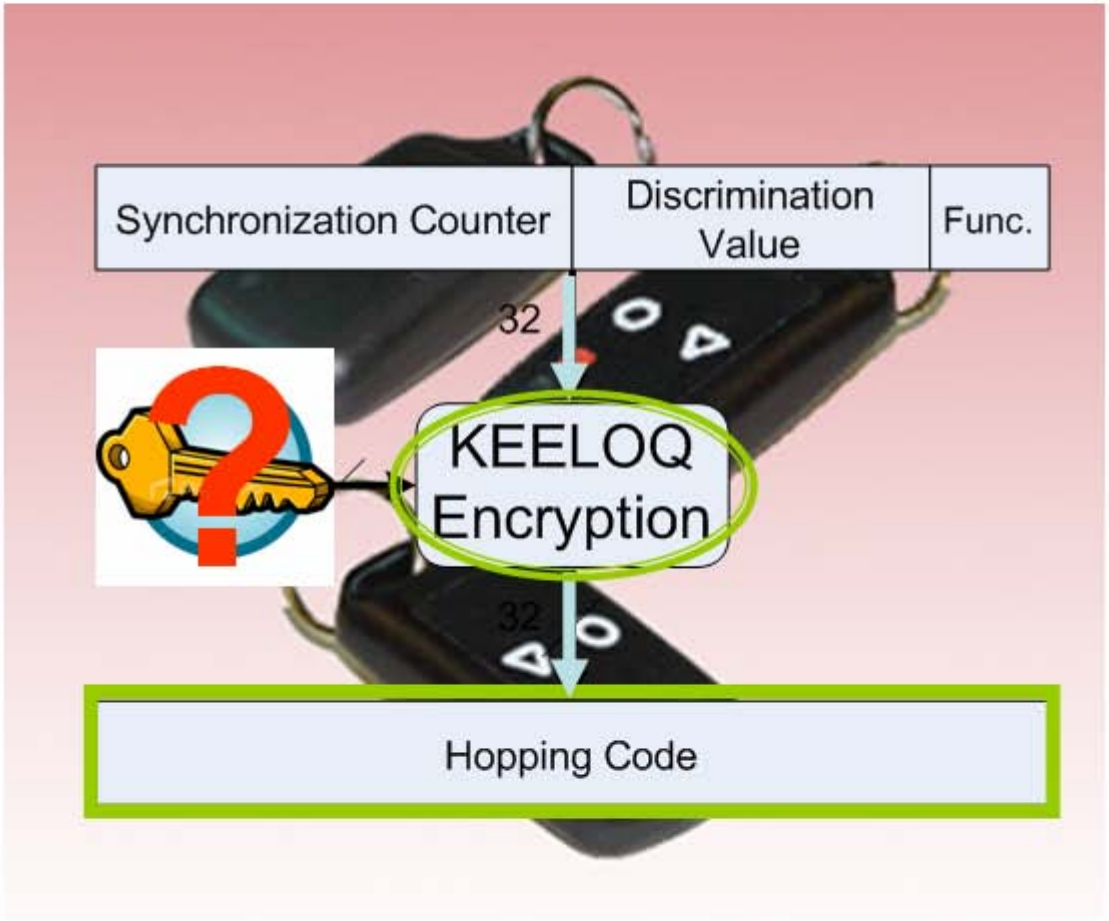
History of Side-Channel Attacks (1-slide version)

Horst-Görtz Institut für IT Sicherheit

- Existence of side-channels for crypto devices known for several decades, (e.g., "Tempest")
- Few concrete results / poor understanding prior to 1996 (at least outside intelligence community)
- 2nd half of 1990s: golden years of SCA
  - RSA CRT attack, 1996
  - Timing attacks, 1996
  - SPA, DPA, 1998
- Since 1999: 100's of SCA research papers, e.g. in CHES
- But: very few (if any) documented real-world attacks

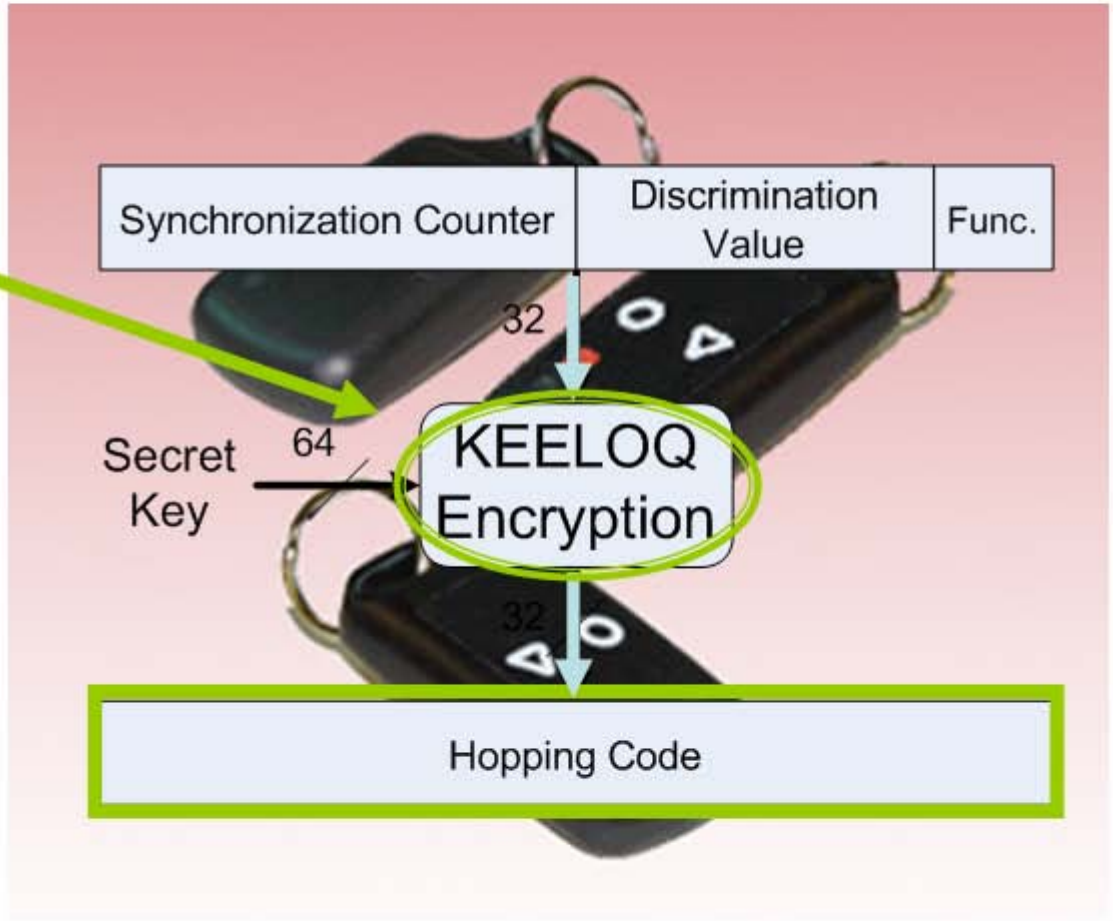
Power Analysis of Remote Control

Horst-Görtz Institut für IT Sicherheit



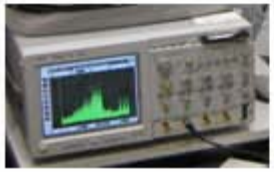
Power Analysis of Remote Control

Horst-Görtz Institut für IT Sicherheit



secret key of remote control (HCS XXX Chip) !

Performing the Side-Channel Attack



Analyze cipher

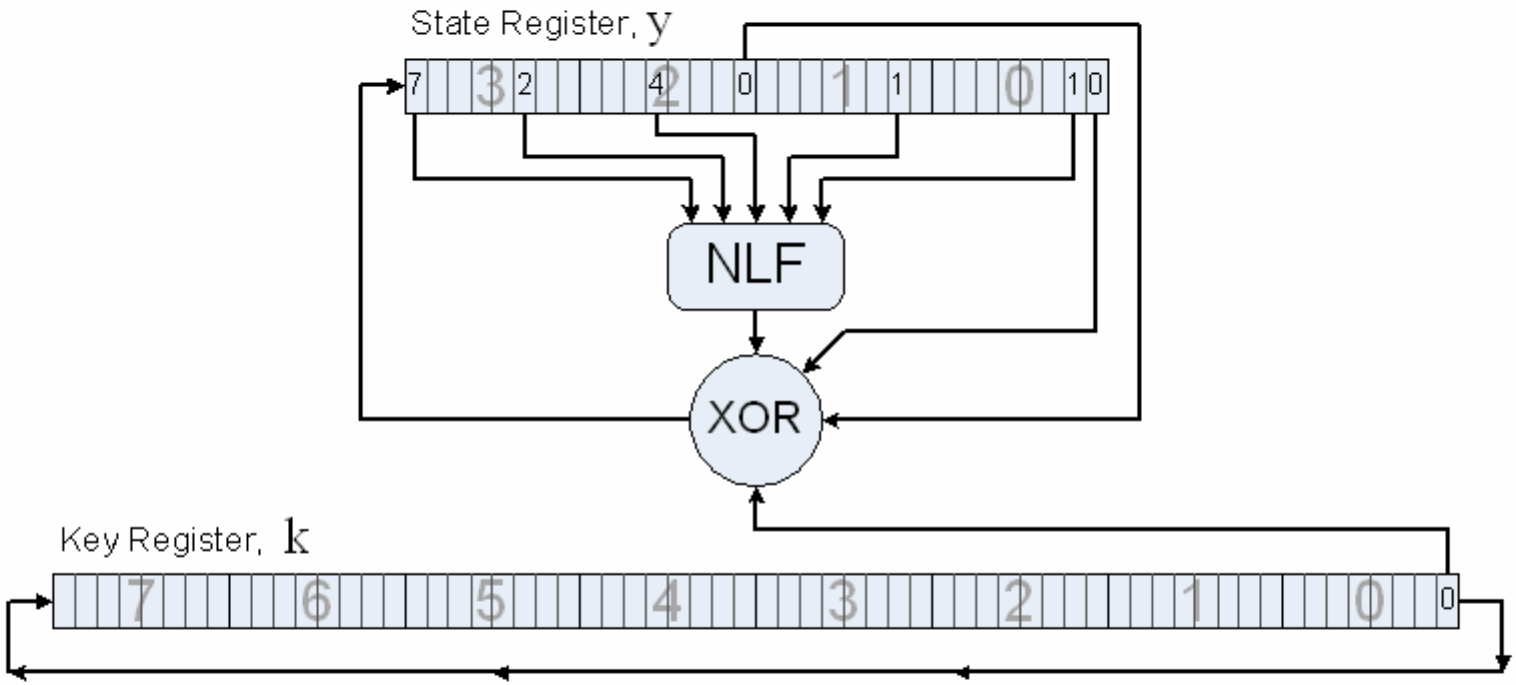
Measurements

Post Processing

Key Recovery

1. Find a suited predictable intermediate value in the cipher
2. Measure the power consumption
3. Align and reduce size of acquired data
4. Correlate measurements with model

KeeLoq – Algorithm

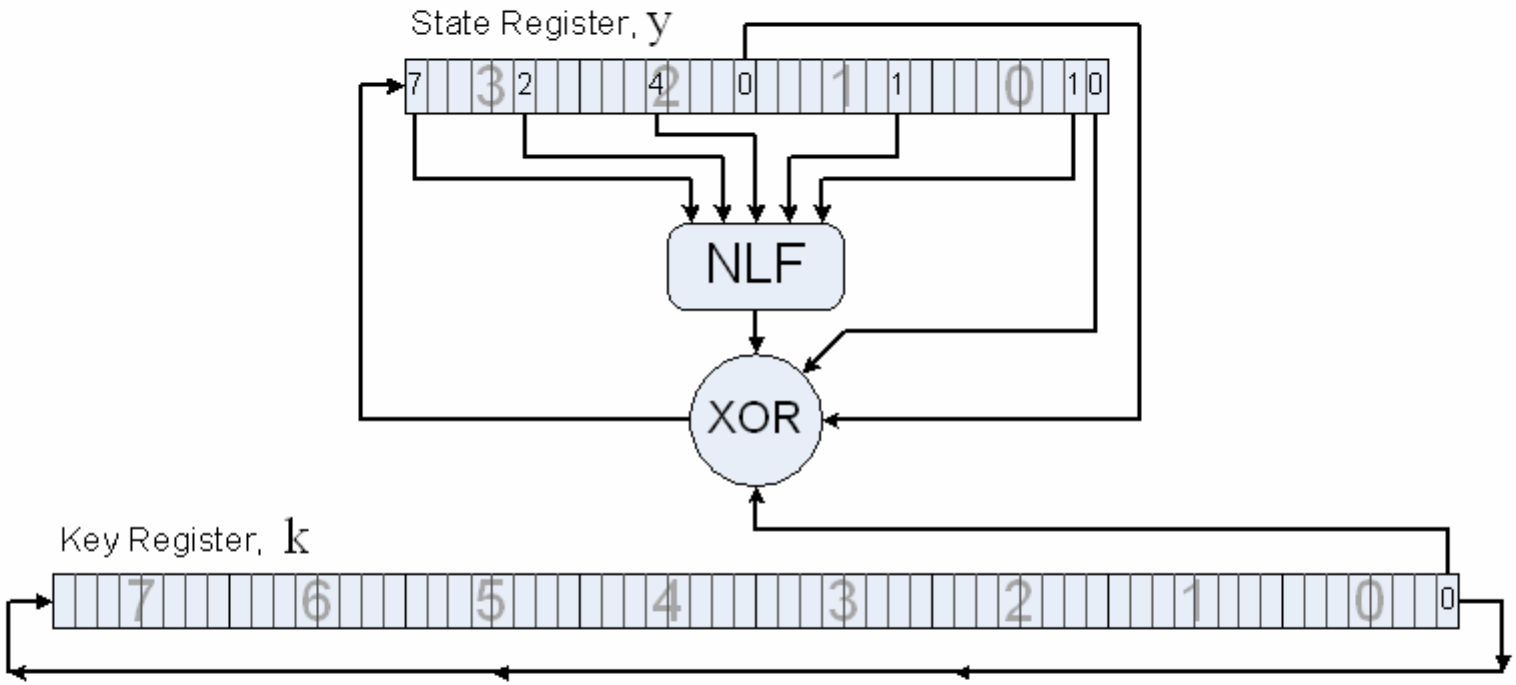


- 64 bit key, 32 bit block length
- NLFSR comprising a 5x1 non-linear function
- Simple key management: key is rotated in every clock cycle
- 528 rounds, each round one key bit is read

→ Lightweight cipher – cheap and efficient in hardware

KeeLoq – Power Model

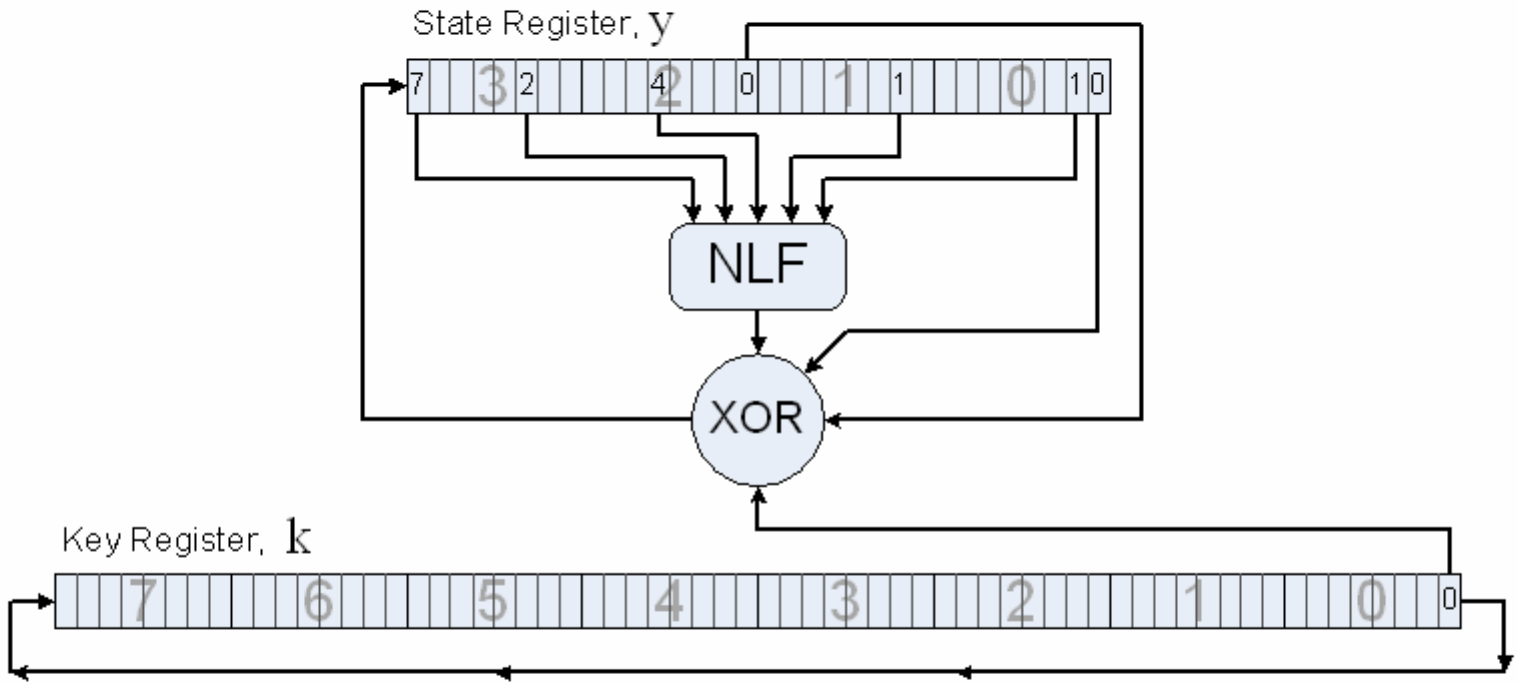
Horst-Görtz Institut
für IT Sicherheit



- Software: typically leaks Hamming weight (HW)
- Hardware: typically leaks Hamming distance (HD)

$$\mathrm{P}_{Hyp}^{(i)} = \mathrm{HD}\left(\boldsymbol{y}^{(i)}, \boldsymbol{y}^{(i-1)}\right) = \mathrm{HW}\left(\boldsymbol{y}^{(i)} \oplus \boldsymbol{y}^{(i-1)}\right)$$

KeeLoq – Power Model

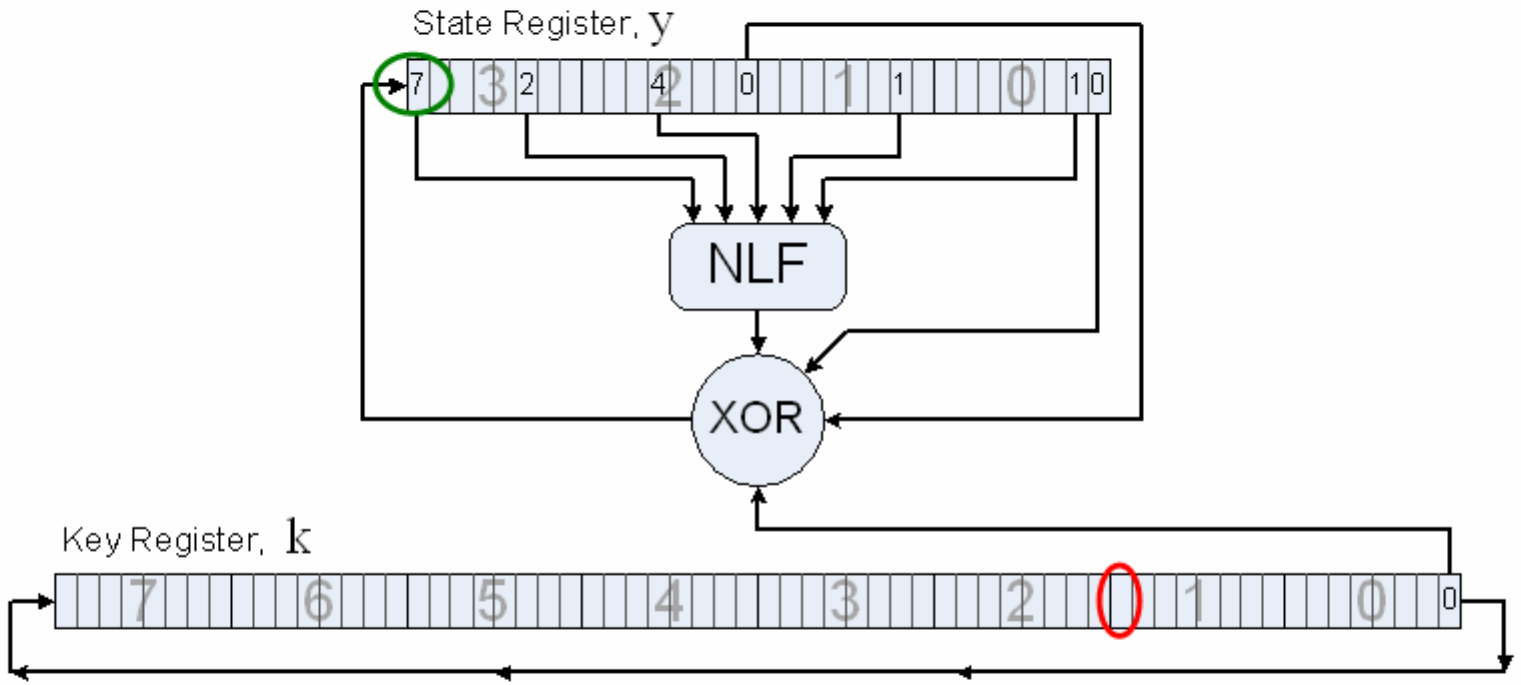


Power Consumption:

- logic is negligible
- depends on number of (toggling) 0s and 1s of the **registers**
- power consumption of Key Register is constant

→ **Variations** of power consumption are related to State Register

KeeLoq – Attack

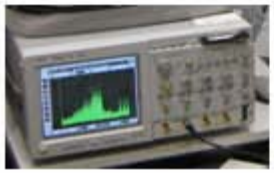


$$y_{31}^{(i+1)} = k_0^{(i)} \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus \mathrm{NLF}\left(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}\right)$$

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

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

Performing the Side-Channel Attack



Analyze cipher

Measurements

Post Processing

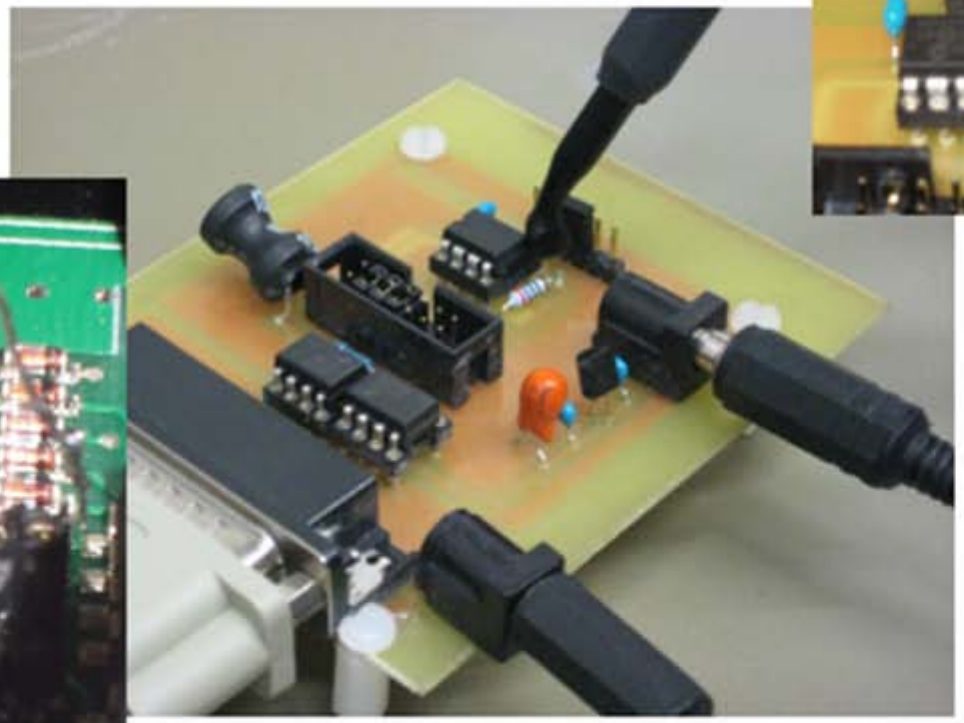
Key Recovery

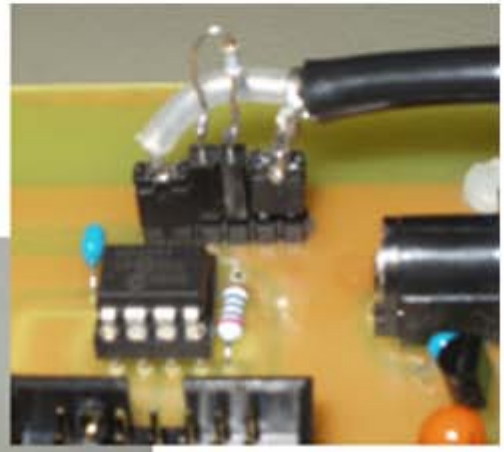
1. Find a suited predictable intermediate value in the cipher
2. Measure the power consumption
3. Align and reduce size of acquired data
4. Correlate measurements with model

Measuring the Power Consumption

Horst-Görtz Institut für IT Sicherheit

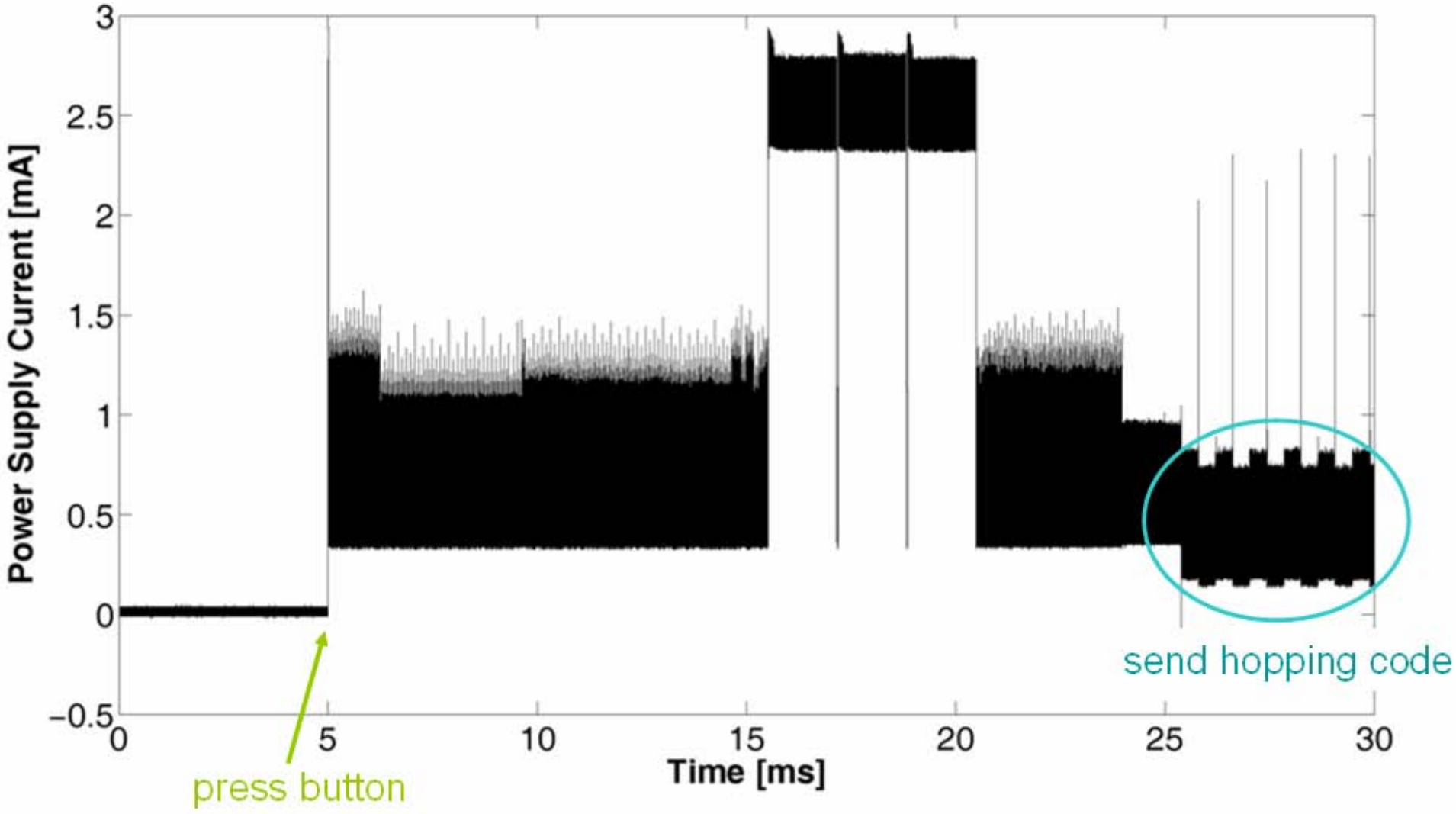
- Digital oscilloscope (max. 1 GS/s sample rate)
- Measure electric current or electromagnetic field



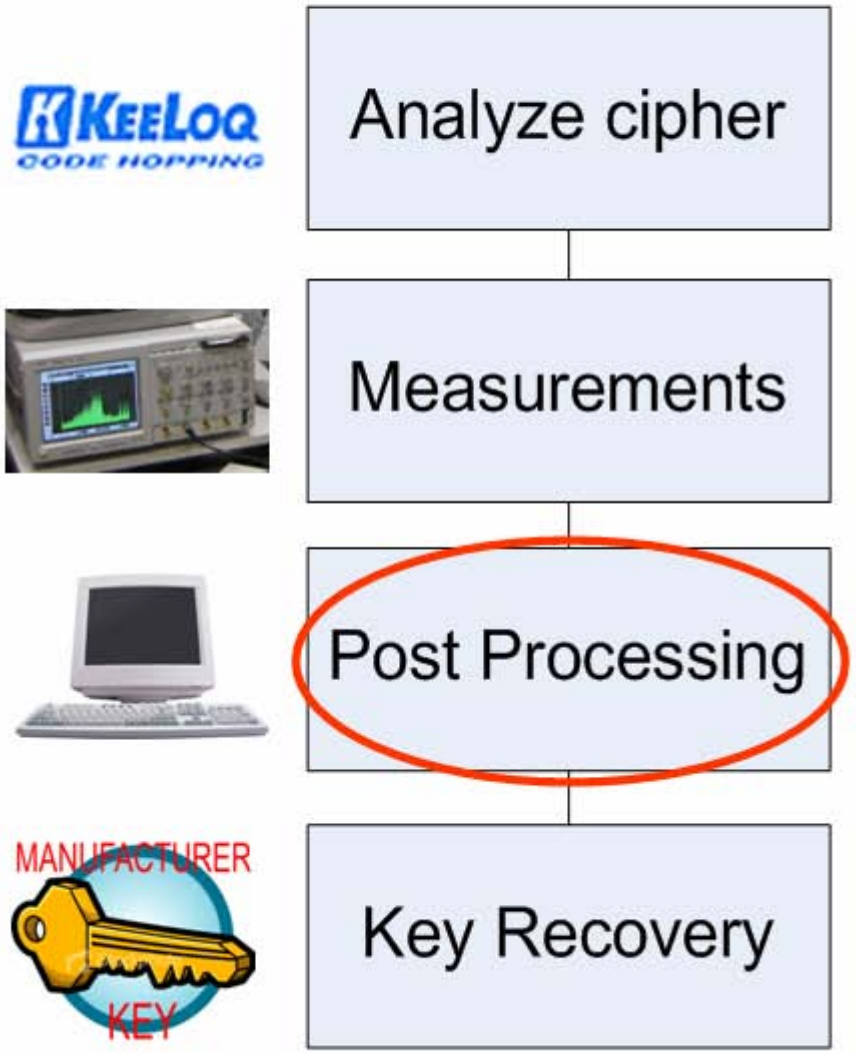


Power Trace of a remote control: Finding the KEELOQ - Encryption

Horst-Görtz Institut für IT Sicherheit



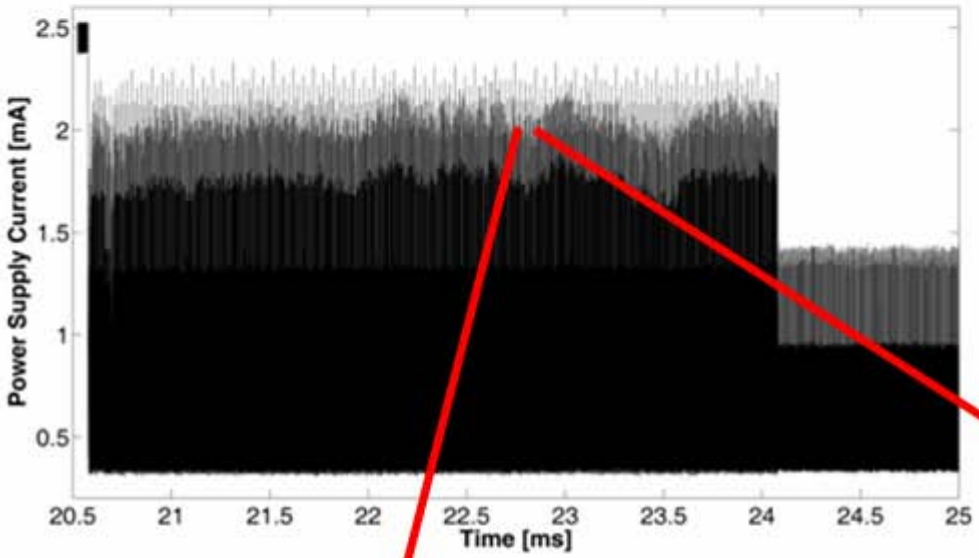
Performing the Side-Channel Attack



1. Find a suited predictable intermediate value in the cipher
2. Perform power measurements
3. Align and reduce size of acquired data
4. Correlate measurements with model

Performing the Side-Channel Attack
Post Processing

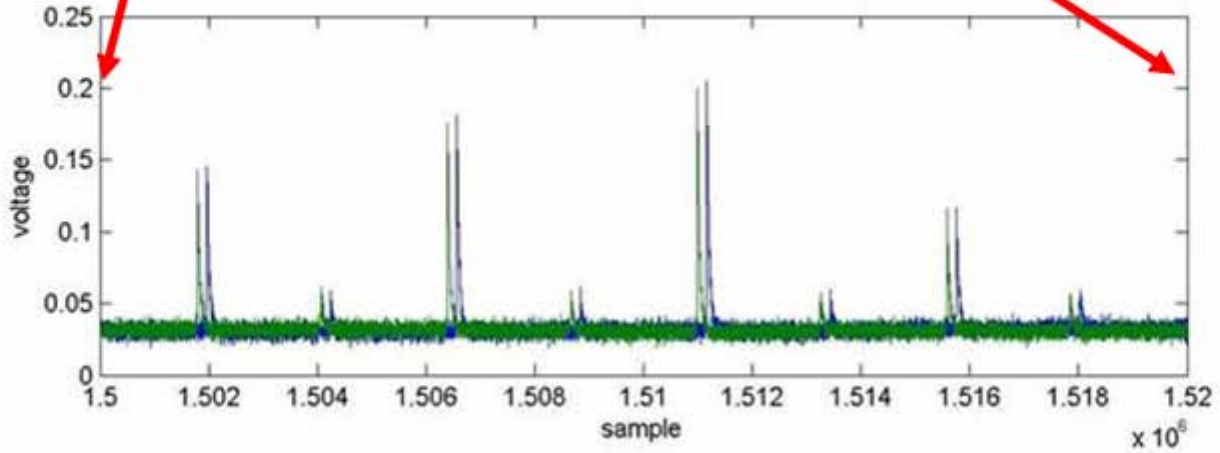
Horst-Görtz Institut
für IT Sicherheit



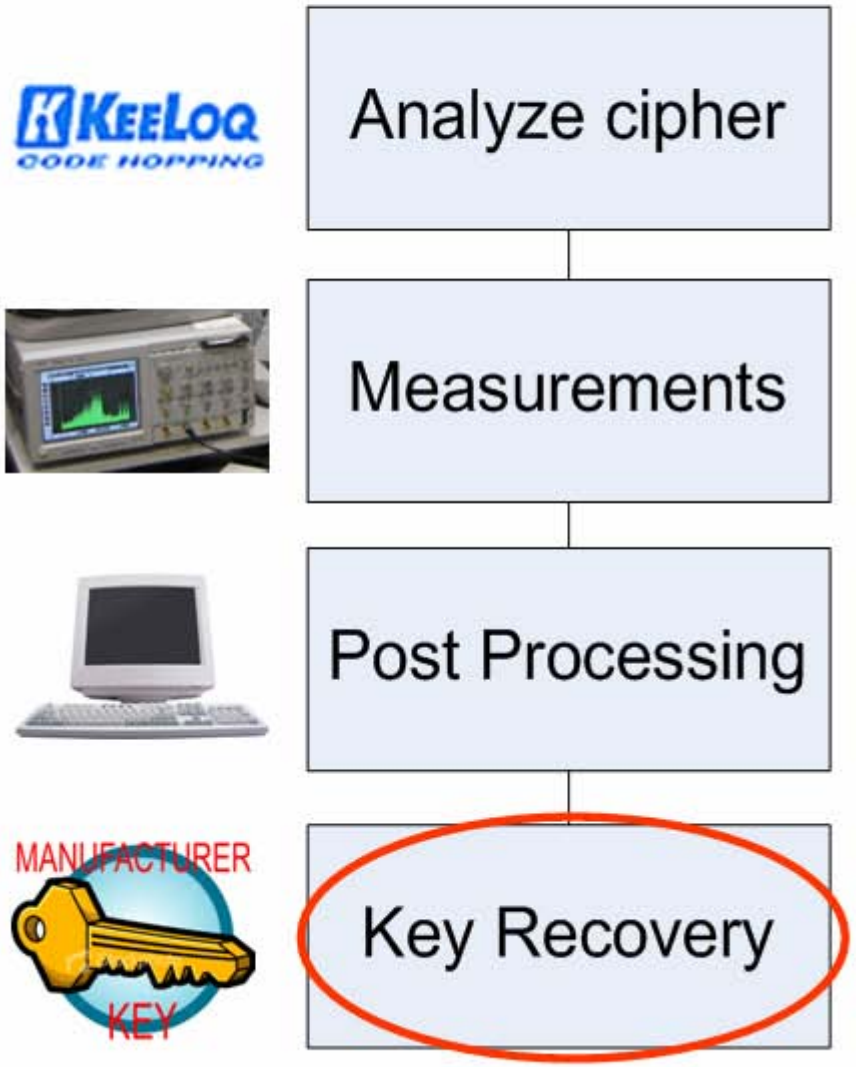
Problems:

- Alignment
- Clock jitter introduces noise
- Traces are very large

Peak detection takes care of **alignment** and **reduces size** of traces!



Performing the Side-Channel Attack

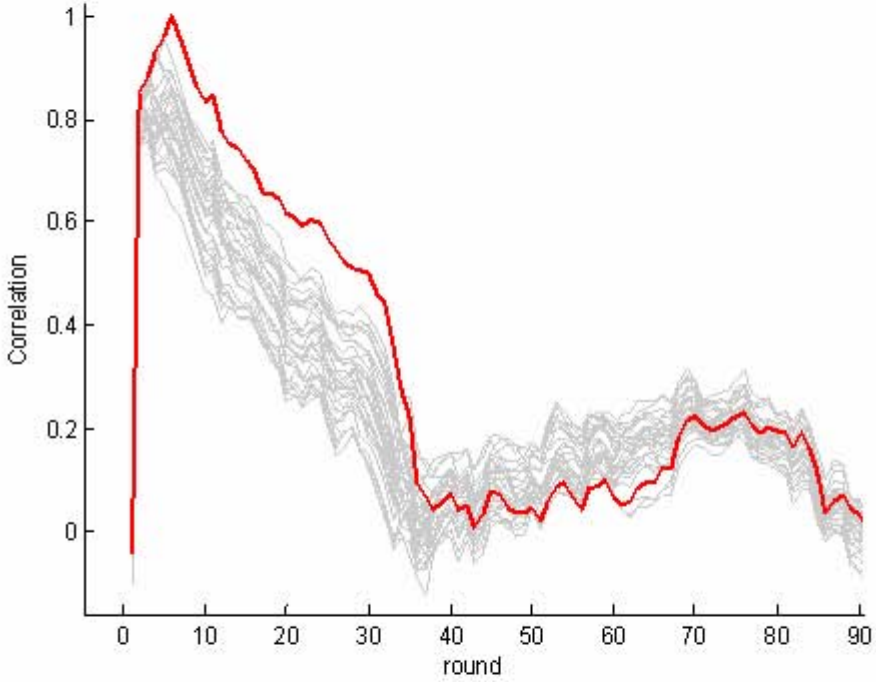


1. Find a suited predictable intermediate value in the cipher
2. Perform power measurements
3. Align and reduce size of acquired data
4. Correlate measurements with model

Performing the Side-Channel Attack
Key Recovery

Horst-Görtz Institut
für IT Sicherheit

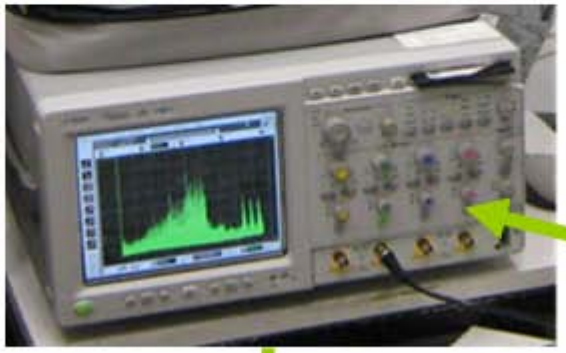
- Correlate power consumption to predicted value $D = f(X_i, K_h)$
- Divide and conquer approach
- Let the best-matching key candidates "survive"

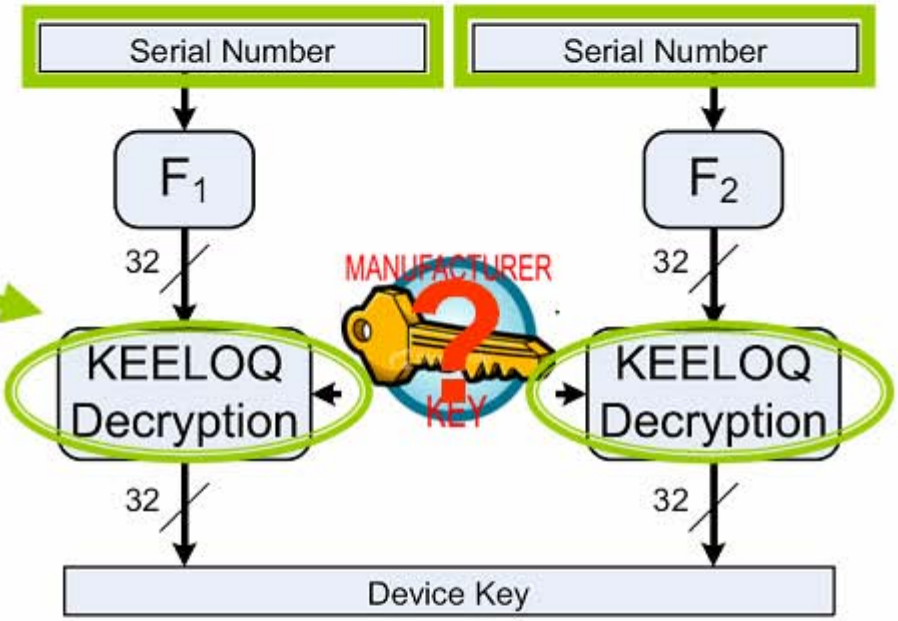


$$r\left(I_i(t), D(X_i, K_h)\right) = \frac{\sum_{i=1}^{M} I_i(t) \cdot D(X_i, K_h)}{\sqrt{\sum_{i=1}^{M}\left(I_i(t) - \overline{I_i(t)}\right)^2 \cdot \sum_{i=1}^{M}\left(D(X_i, K_h) - \overline{D(X_i, K_h)}\right)^2}} - \frac{\frac{1}{M} \cdot \sum_{i=1}^{M} I_i(t) \cdot \sum_{i=1}^{M} D(X_i, K_h)}{\sqrt{\sum_{i=1}^{M}\left(I_i(t)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

Power Analysis of the Receiver

Horst-Görtz Institut
für IT Sicherheit





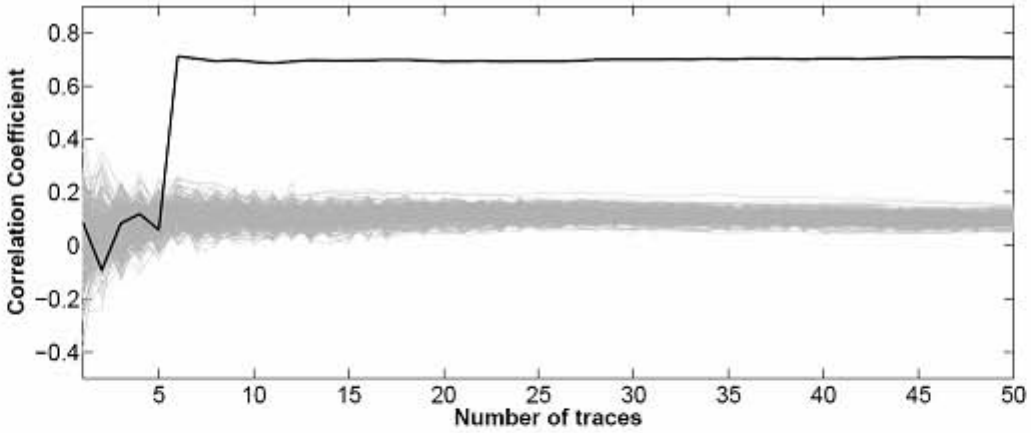
secret key of manufacturer!

Side-Channel Attack Results for KeeLoq

Horst-Görtz Institut für IT Sicherheit

A) Hardware implementation ("car key")

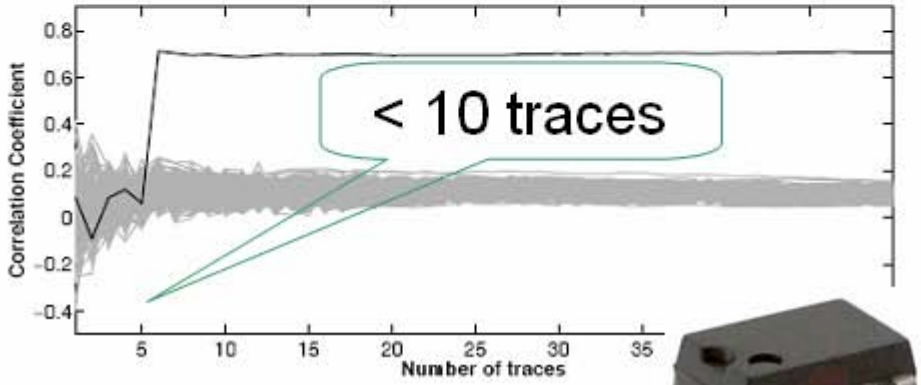
- Total attack time (for known device family):
  5-30 traces, ≈ minutes



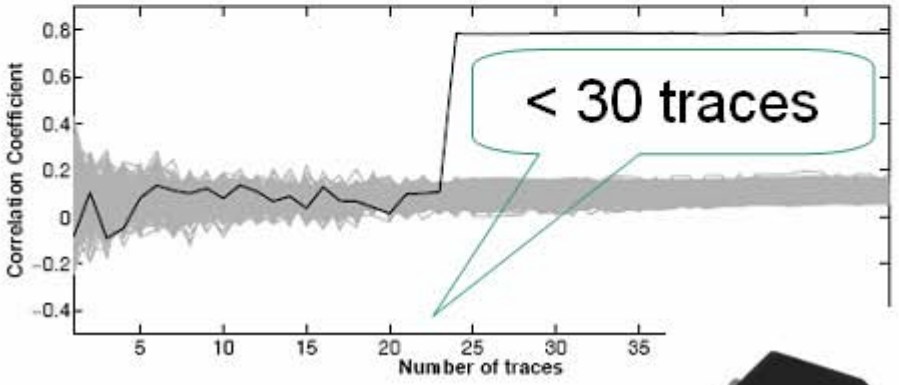
B) Software implementation ("car door")

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

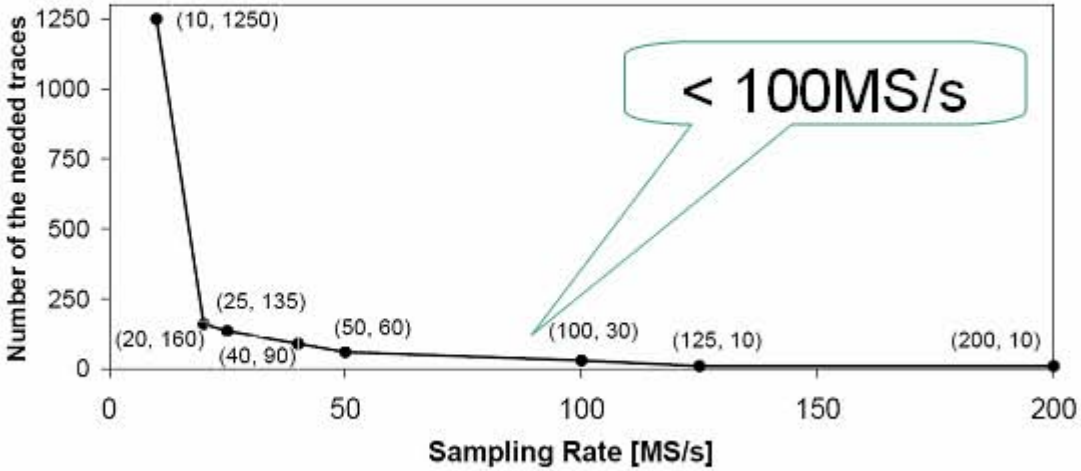
Comparison of Packages & Sample Rates



(a) DIP



(b) SOIC



No expensive equipment needed for key recovery !

So what can we do now (1) ?

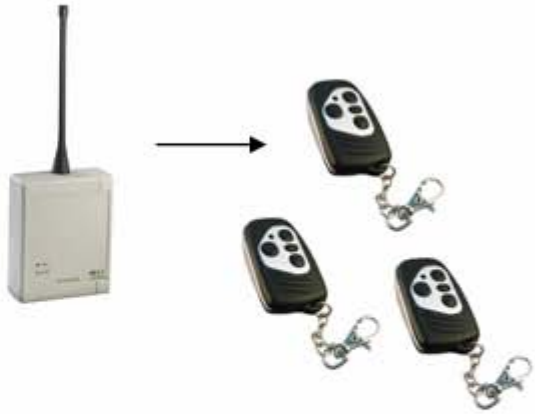
Horst-Görtz Institut für IT Sicherheit

1. If we have access to a remote:

   Recover Device Key and clone the remote

2. If we have access to a receiver:

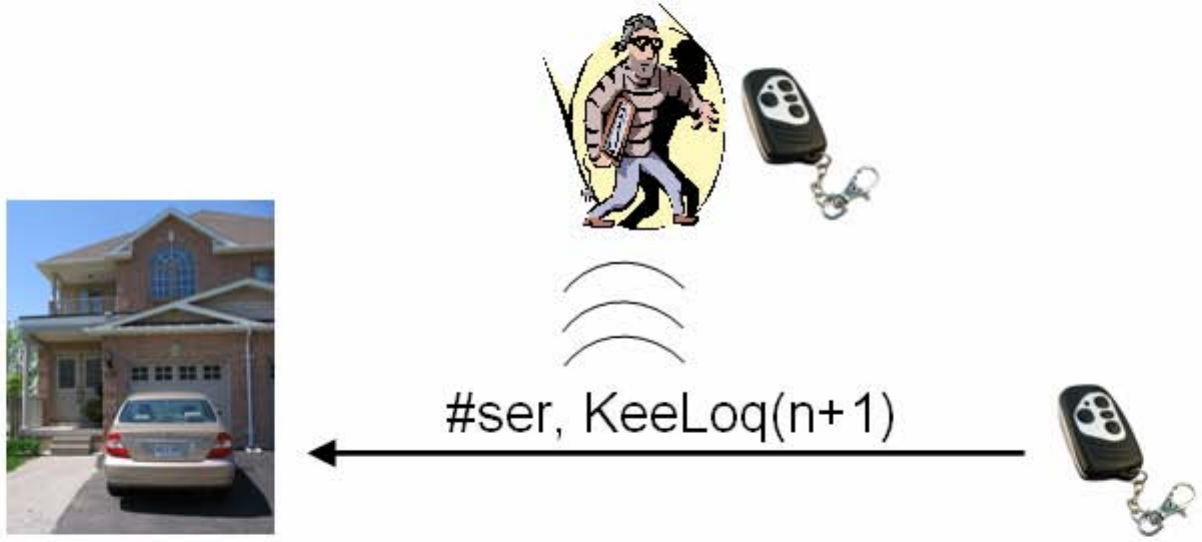
   Recover Manufacturer Key & generate new remotes



So what can we do now (2) ?

Horst-Görtz Institut für IT Sicherheit

3. After step 2 (i.e., possessing the Manufacturer Key):
   Remotely eavesdrop on 1-2 communications & clone remote!



www.copacobana.org

- works for all key derivation schemes
- **instantly** for key derivation from serial number
- otherwise use PC (short seed) or COPACOBANA (long seed)

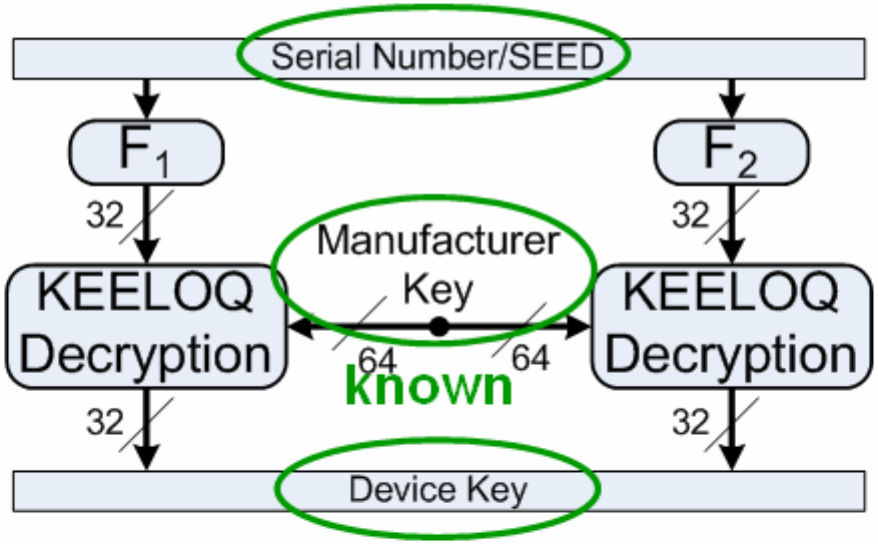
Details on Eavesdropping Attack

Horst-Görtz Institut für IT Sicherheit

Possessing the Manufacturer Key:

Remotely eavesdrop on 1-2 communications, and clone Device Key!

known(Serial) or brute-forced(Seed)



…easy.

1. Recover Device Key
2. Decrypt Rolling Code → obtain counter etc.
3. Clone the remote control

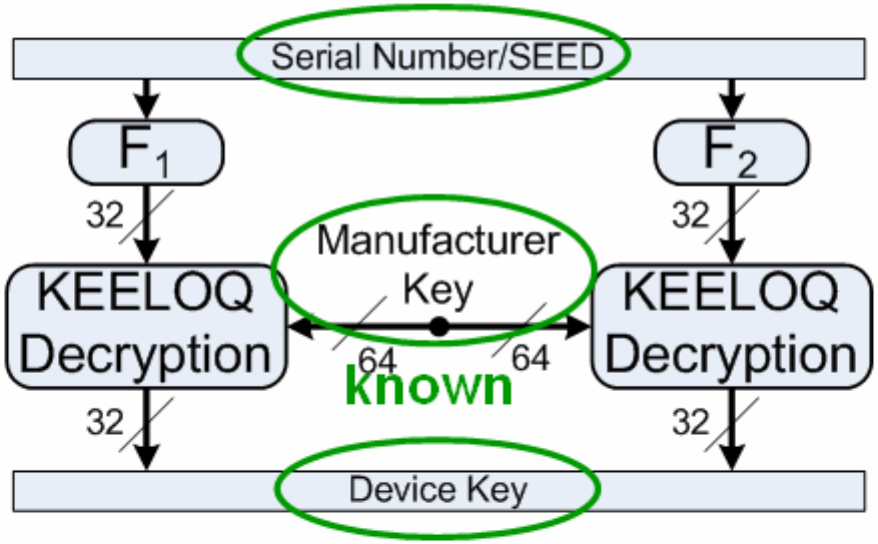
Details on Eavesdropping Attack

Horst-Görtz Institut für IT Sicherheit

Possessing the Manufacturer Key:

Remotely eavesdrop on 1-2 communications, and clone Device Key!

known(Serial) or brute-forced(Seed)



...easy.

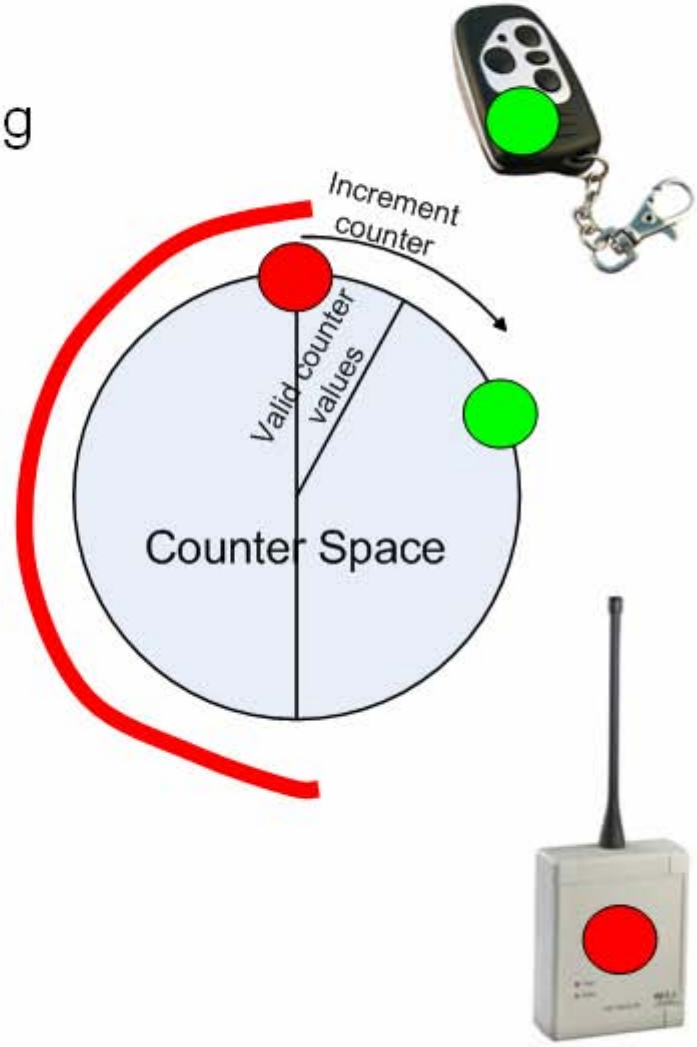
Side-channel step (one-time recovery of manufacturer key), difficult, can be outsourced to criminal cryptographers !

Taking over a KeeLoq System

Horst-Görtz Institut für IT Sicherheit

- Receiver updates its internal counter according to the last received valid Rolling Code

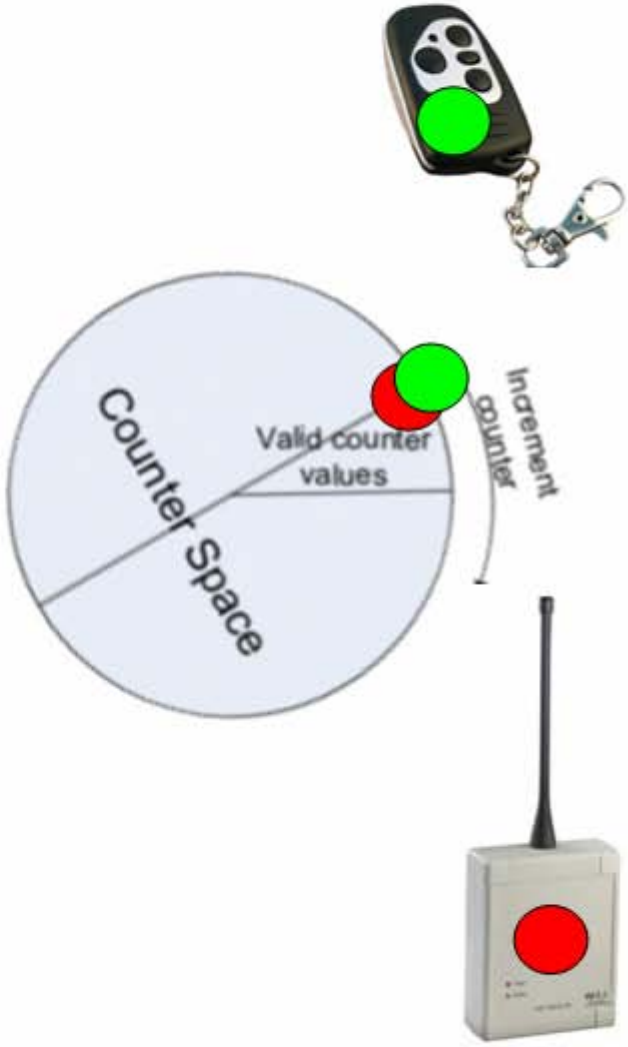
Block Window



Taking over a KeeLoq System

Horst-Görtz Institut für IT Sicherheit

- Receiver updates its internal counter according to the last received valid Rolling Code



Taking over a KeeLoq System

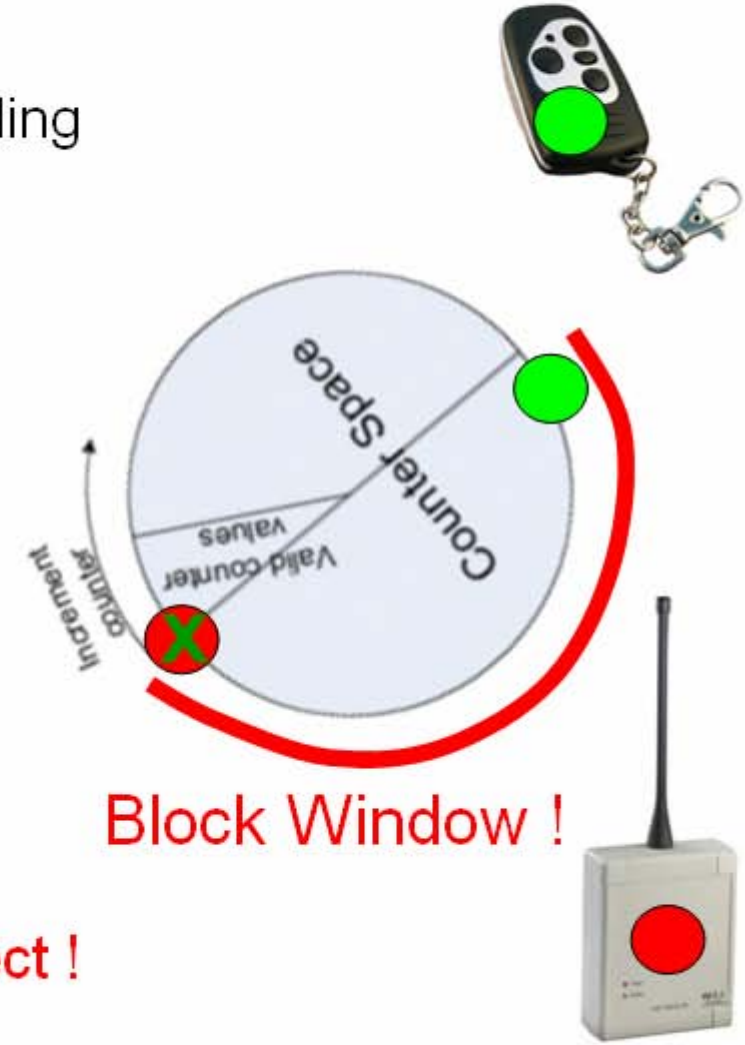
Horst-Görtz Institut für IT Sicherheit

- Receiver updates its internal counter according to the last received valid Rolling Code

- Generate valid Rolling Code with chosen counter value

- Counter of original remote control is in the block window → Door will not open.

- Attacker can still access the secured object !



Summary

Horst-Görtz Institut für IT Sicherheit

- "Security by Obscurity" makes insecure systems
- DPA works for commercial access control system
- some severe attacks can be done by non-specialists

- side-channel attacks are a real threat for **all** unprotected implementations of cryptography (ECC, AES, …)
- we have to put SCA-resistance in many devices, including embedded / consumer-style applications

Disclaimer: Our attacks do **not** imply that real-world systems have actually been attacked via SCA by criminals (merely by researchers).

Literature

T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer, 2008.

A. Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. In *3rd Conference on RFID Security 2007 (RFIDSec 2007)*. `http://rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf`.

N. T. Courtois, G. V. Bard, and D. Wagner. Algebraic and Slide Attacks on KeeLoq. In *Fast Software Encryption - FSE 2008*, Lecture Notes in Computer Science. Springer, 2008.

S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A Practical Attack on KeeLoq. In *Advances in Cryptology - EUROCRYPT 2008*, Lecture Notes in Computer Science. Springer, 2008.

Timo Kasper

contact: *tkasper@crypto.rub.de*

Embedded Security Group (C. Paar)
Ruhr-University Bochum
www.crypto.rub.de