On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme

CRYPTO 2008

August 17-21, 2008

Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar,
Mahmoud Salmasizadeh, Mohammad T. Manzuri Shalmani

www.crypto.rub.de

Acknowledgement

We would like to thank Andrey Bogdanov for bringing KeeLoq to our attention and for many helpful discussions.

Contents

Horst-Görtz Institut für IT Sicherheit

1. Background
2. KeeLoq block cipher
3. Side-channel attacking KeeLoq
4. Results

Contents

Horst-Görtz Institut für IT Sicherheit

1. **Background**
2. KeeLoq block cipher
3. Side-channel attacking KeeLoq
4. Results

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

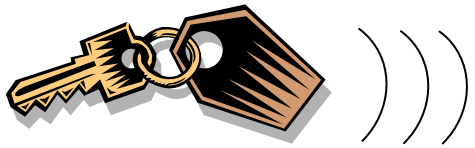
Horst-Görtz Institut für IT Sicherheit

- 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 to date

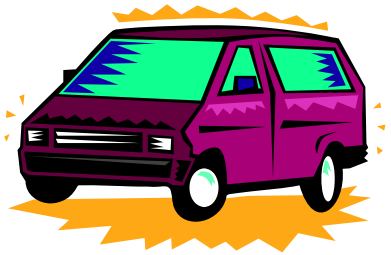
Modern Keyless Entry Systems: Hopping Code (aka Rolling Code)

Horst-Görtz Institut für IT Sicherheit

advanced theft control: rolling code



code = $e_k(n_i)$



$e_k()$ is often a block cipher

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

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

....

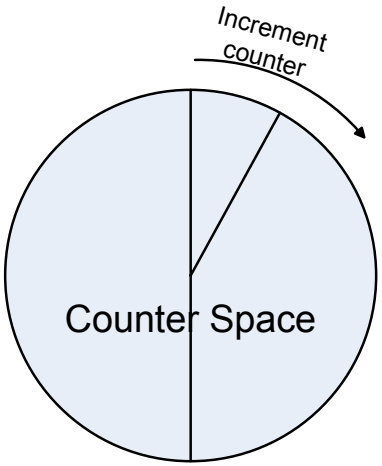
Alternatively, challenge-response protocols can be used
(but require bidirectional channel)

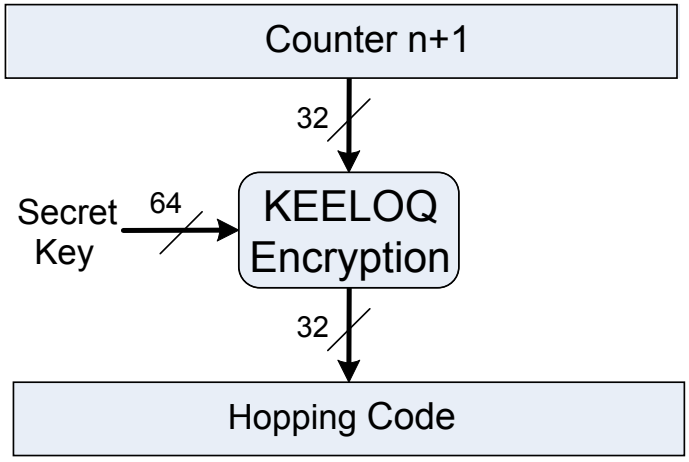
Contents

Horst-Görtz Institut für IT Sicherheit

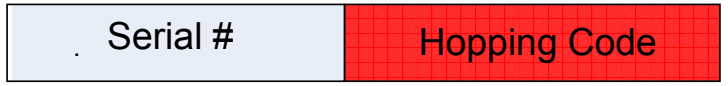
1. Background
2. **KeeLoq block cipher**
3. Side-channel attacking KeeLoq
4. Results

KeeLoq Rolling Code Scheme





Receiver decrypts & checks validity of counter value

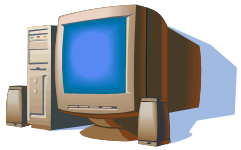


KeeLoq Key Management

Horst-Görtz Institut für IT Sicherheit

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} = KeeLoq(#ser, k_M)

Key derivation

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

#ser

k_M

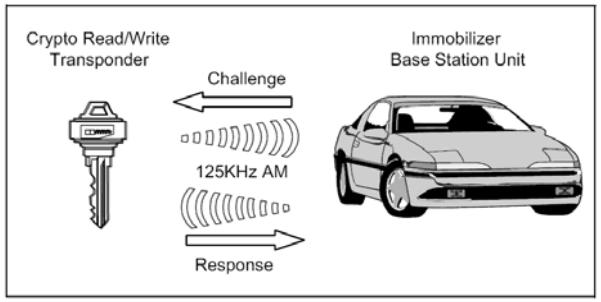
1. computes k_{dev} = KeeLoq(#ser, k_M)
2. stores (#ser , k_{dev})

Remark: simple XOR-based key derivation also possible

KeeLoq Applications

Horst-Görtz Institut
für IT Sicherheit

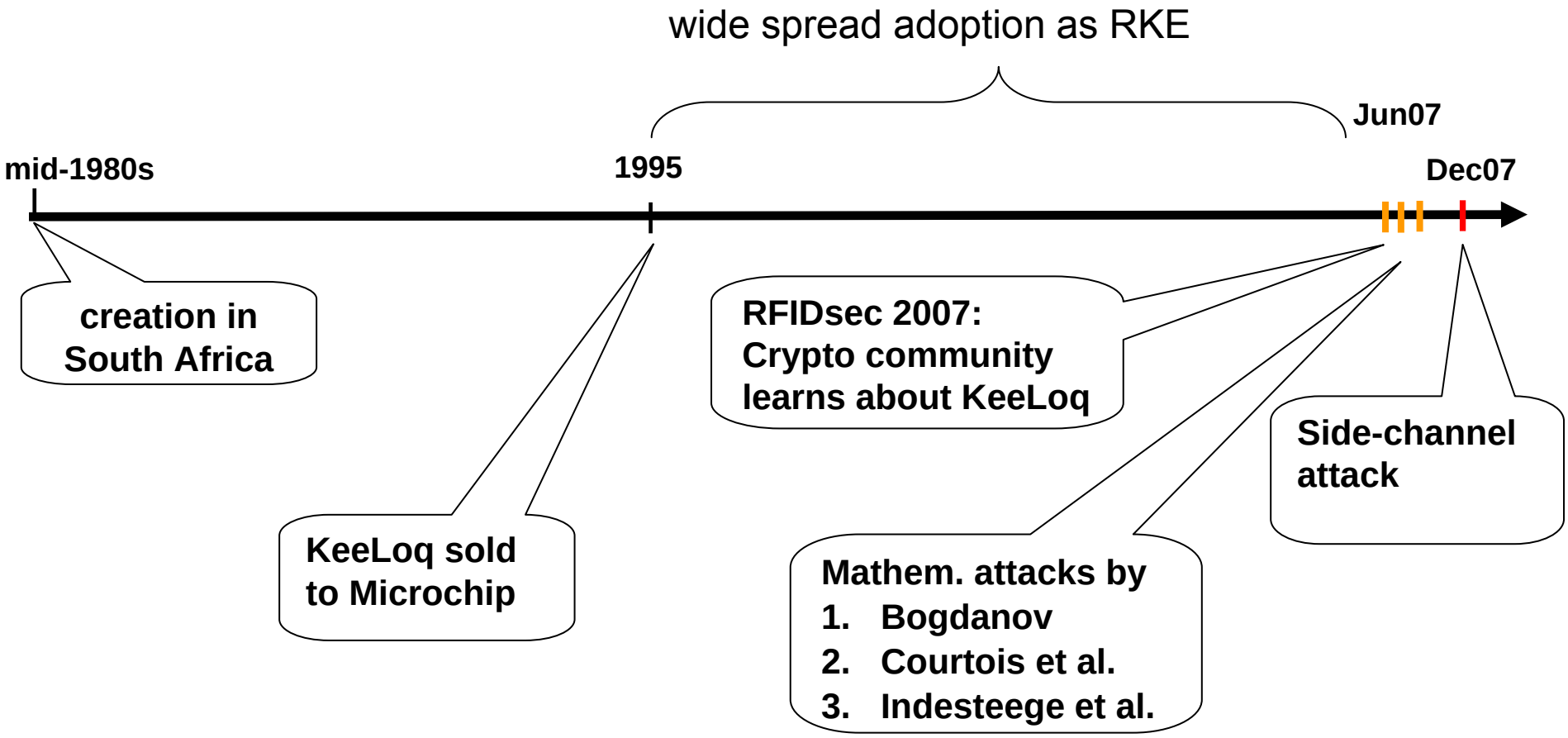
HCS410 IMMOBILIZER TRANSPONDER



- automotive and building access authentication
- KeeLoq implemented in hardware (transmitter) or software (receiver)
- can be used as rolling code or challenge-response
- very widely used for **garage doors** in US and Europe
- Wikipedia (?) Car door opening: Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Jaguar, ...

Q: How secure is KeeLoq?

Rise and Fall of KeeLoq



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 attack (sliding attack) is 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?**

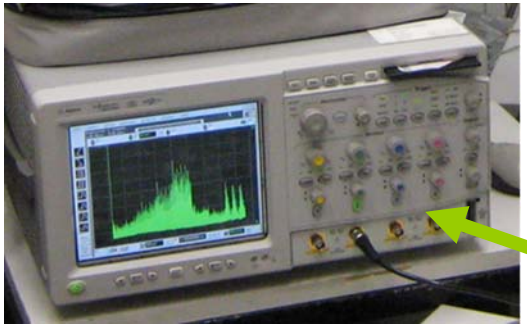
Contents

Horst-Görtz Institut für IT Sicherheit

1. Background
2. KeeLoq block cipher
3. **Side-channel attacking KeeLoq**
4. Results

Side Channel Analysis

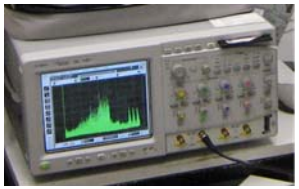
Horst-Görtz Institut für IT Sicherheit



secret key of remote control (HCS XXX Chip) !

Performing the Side Channel Attack

Horst-Görtz Institut für IT Sicherheit



Analyze cipher

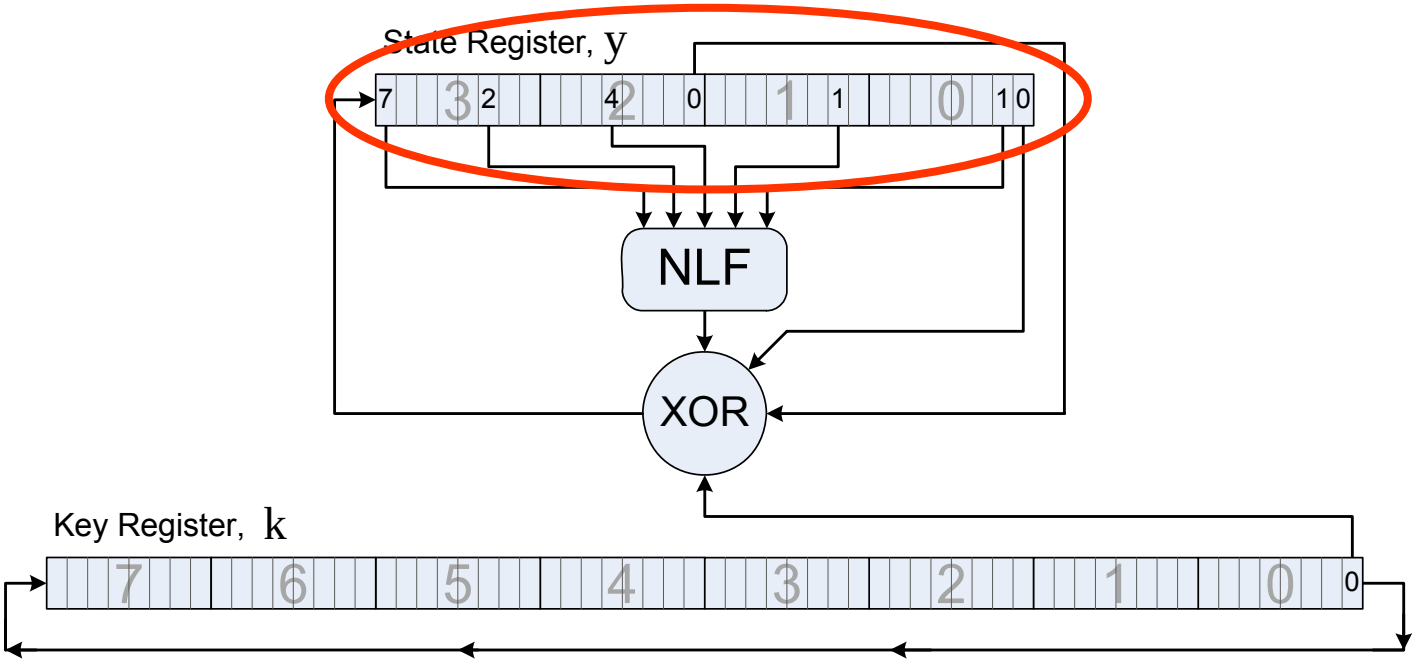
Measurements

Post Processing

Key Recovery

1. Find a suited predictable intermediate value in the cipher
2. Perform power measurements
3. Post-process acquired data
4. Perform the attack to recover the key

KeeLoq – The Algorithm



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

Power Consumption:

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

→ **Changes** in power consumption is related to state which leaks key information

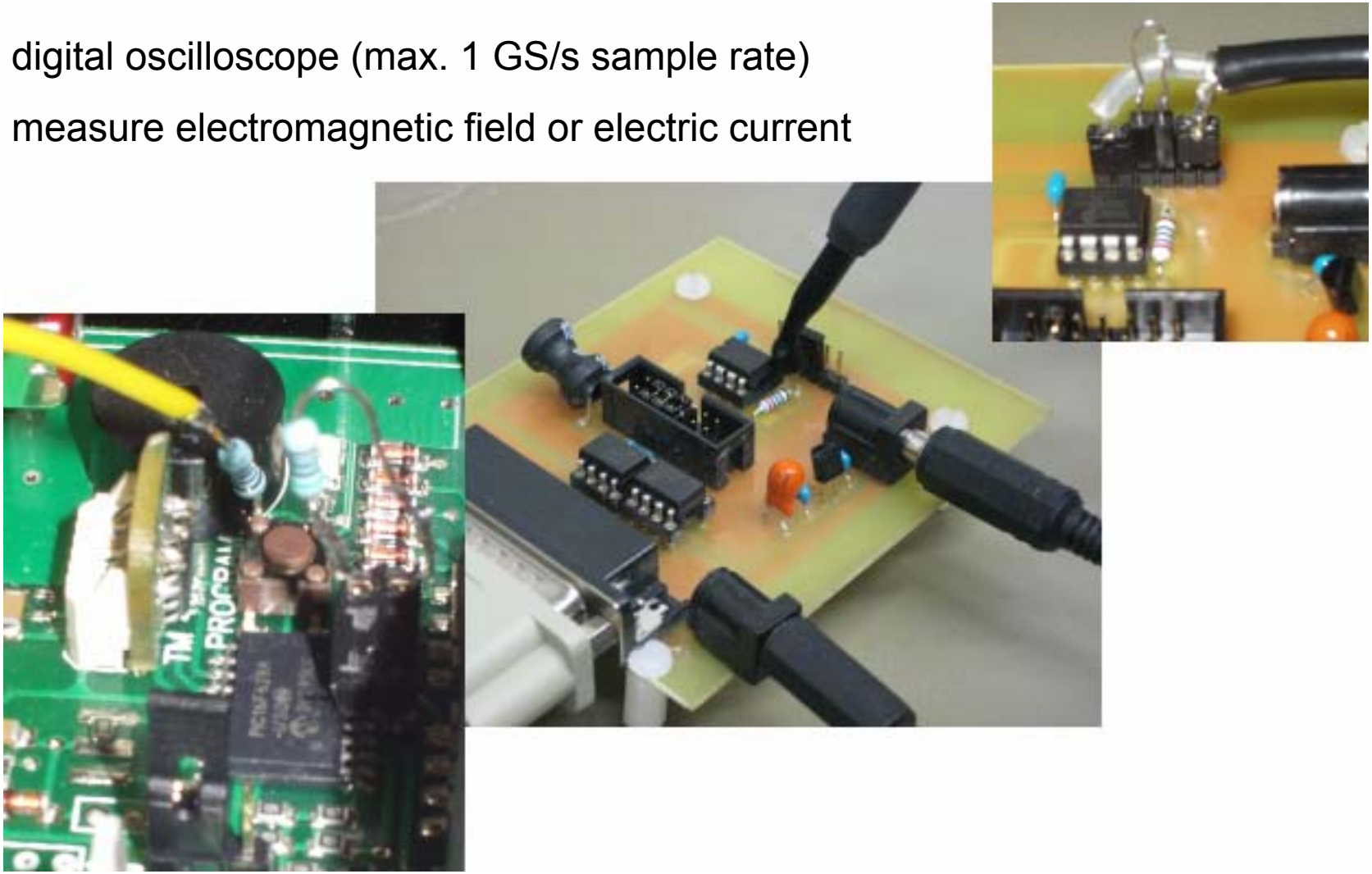
Performing the Side-Channel Attack

1. Find a suited predictable intermediate value in the cipher
2. Perform power measurements
3. Post-process acquired data
4. Perform the attack to recover the key

Measuring the Power Consumption

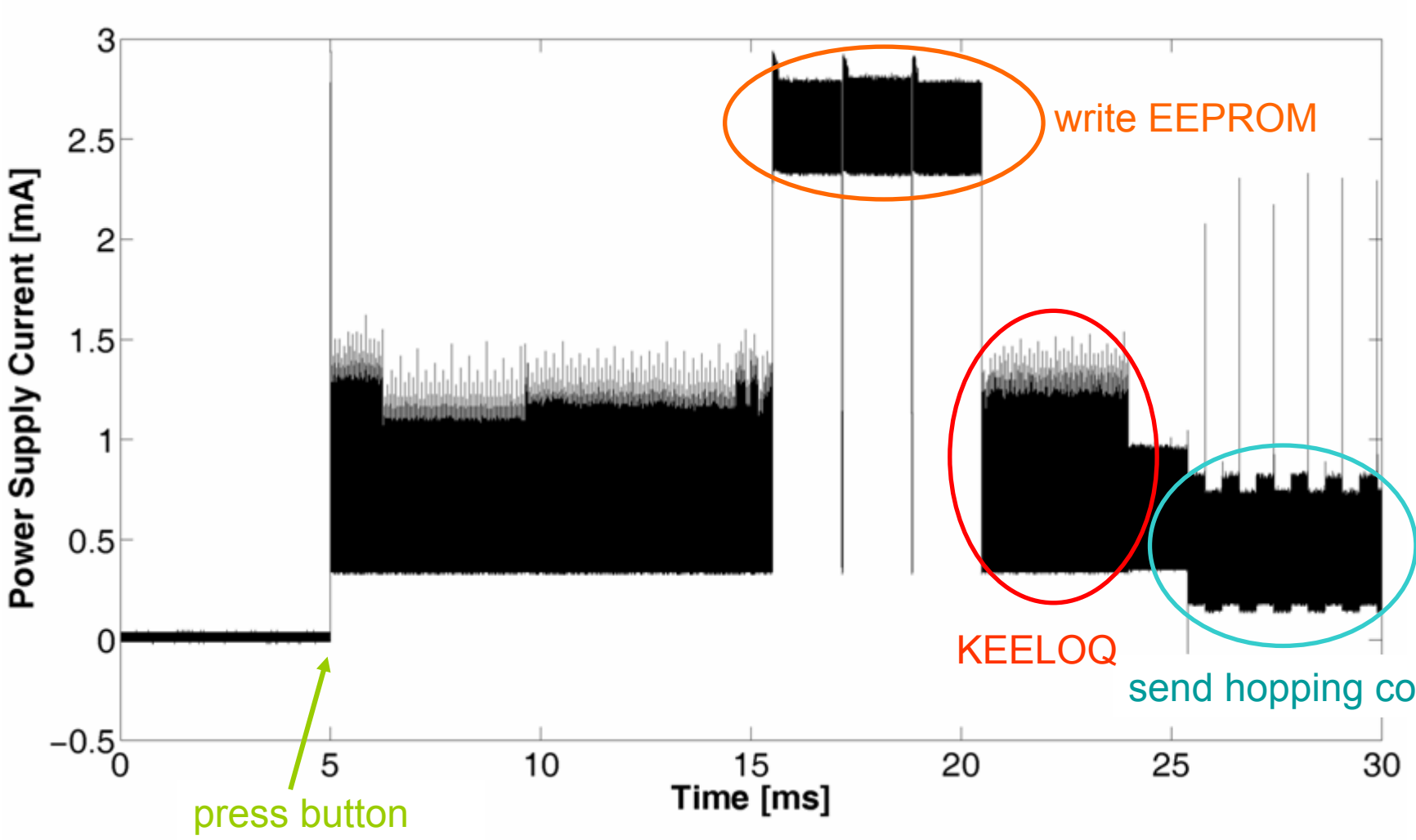
Horst-Görtz Institut für IT Sicherheit

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



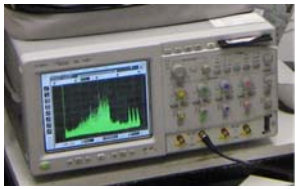
Identifying the KEELOQ - Encryption

Horst-Görtz Institut für IT Sicherheit



Performing the Side-Channel Attack

Horst-Görtz Institut für IT Sicherheit



Analyze cipher

Measurements

Post Processing

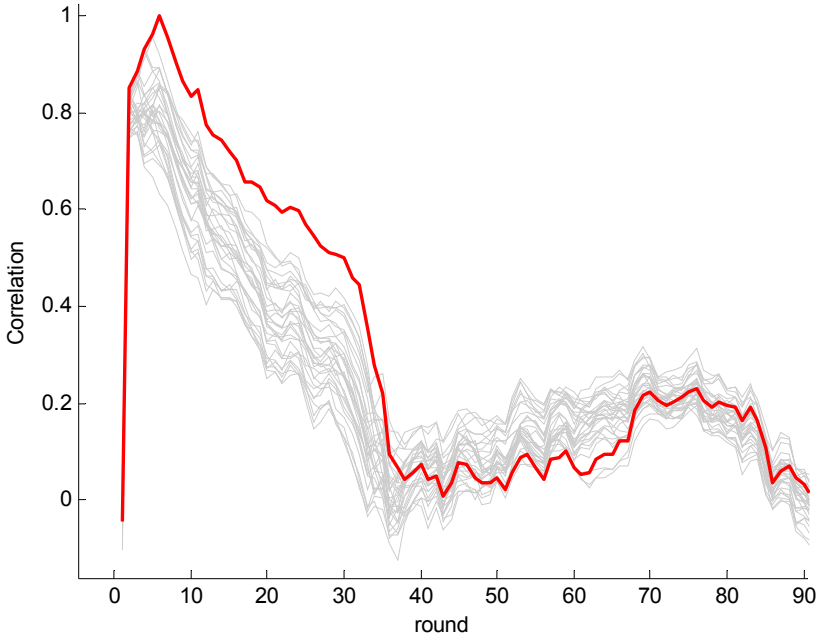
Key Recovery

1. Find a suited predictable intermediate value in the cipher
2. Perform power measurements
3. Post-process acquired data
4. Perform the attack to recover the key

Performing the Side-Channel Attack
Key Recovery

Horst-Görtz Institut für IT Sicherheit

- Correlate measured power consumption to predicted key-dependent value y = f(x,k)
- Divide and conquer approach
- Much off-line number crunching



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

Contents

Horst-Görtz Institut für IT Sicherheit

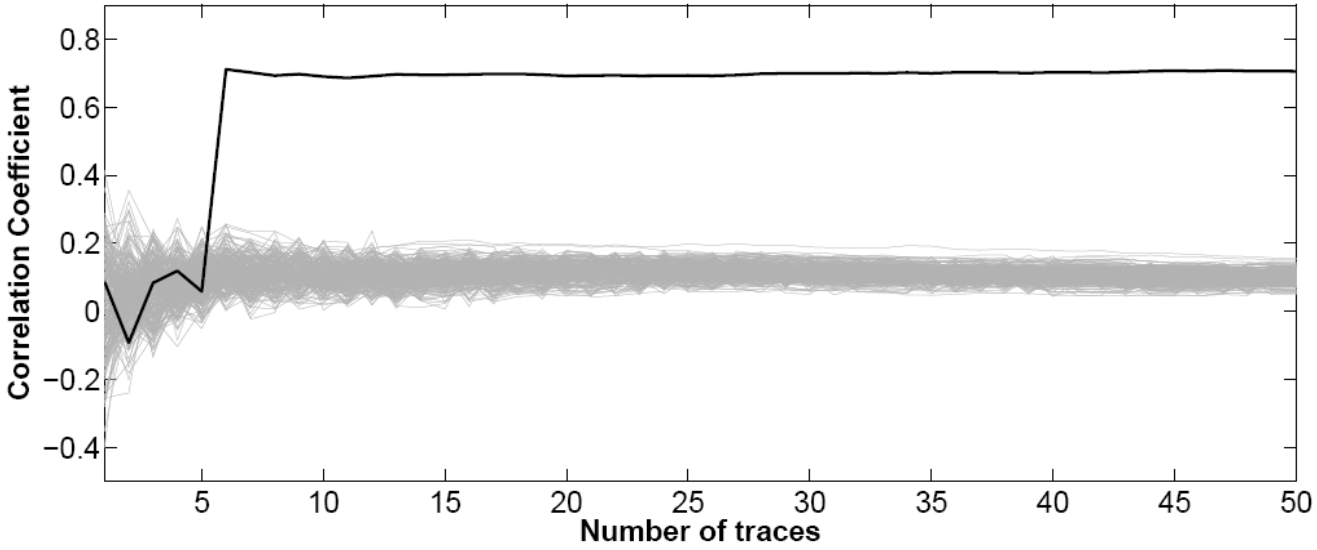
1. Background
2. KeeLoq block cipher
3. Side-channel attacking KeeLoq
4. **Results**

Side Channel Attack on transmitters

Horst-Görtz Institut für IT Sicherheit

KeeLoq implemented in hardware

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



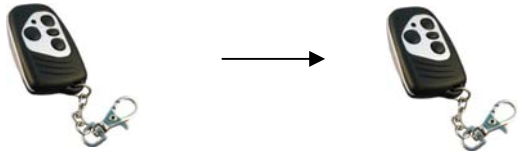
Convergence of correlation coefficient

Rem: low cost equipment suffices (< $1000)

So what can we do now (1) ?

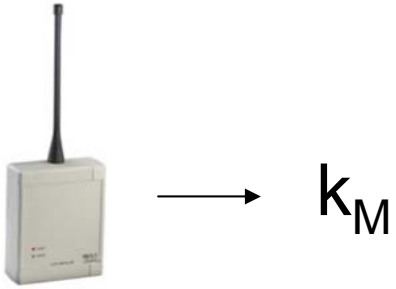
Horst-Görtz Institut für IT Sicherheit

1. If we have access to a remote:



   Recover device key and clone the device

2. If we have access to a receiver:

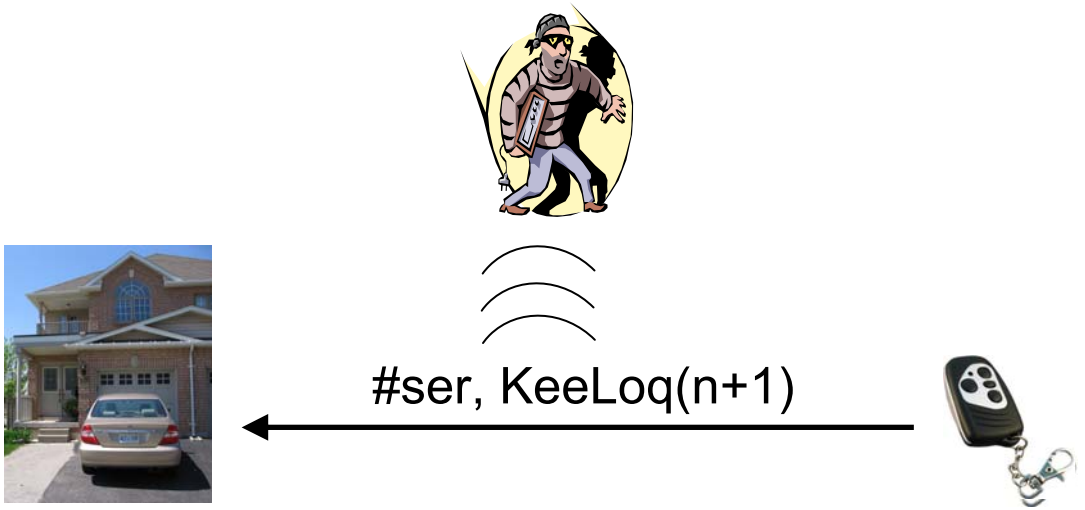


   Recover manufacturer key

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 !**

Thanks for your attention!

more info: www.crypto.rub/keeloq

DOS - Denial Of Service

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.