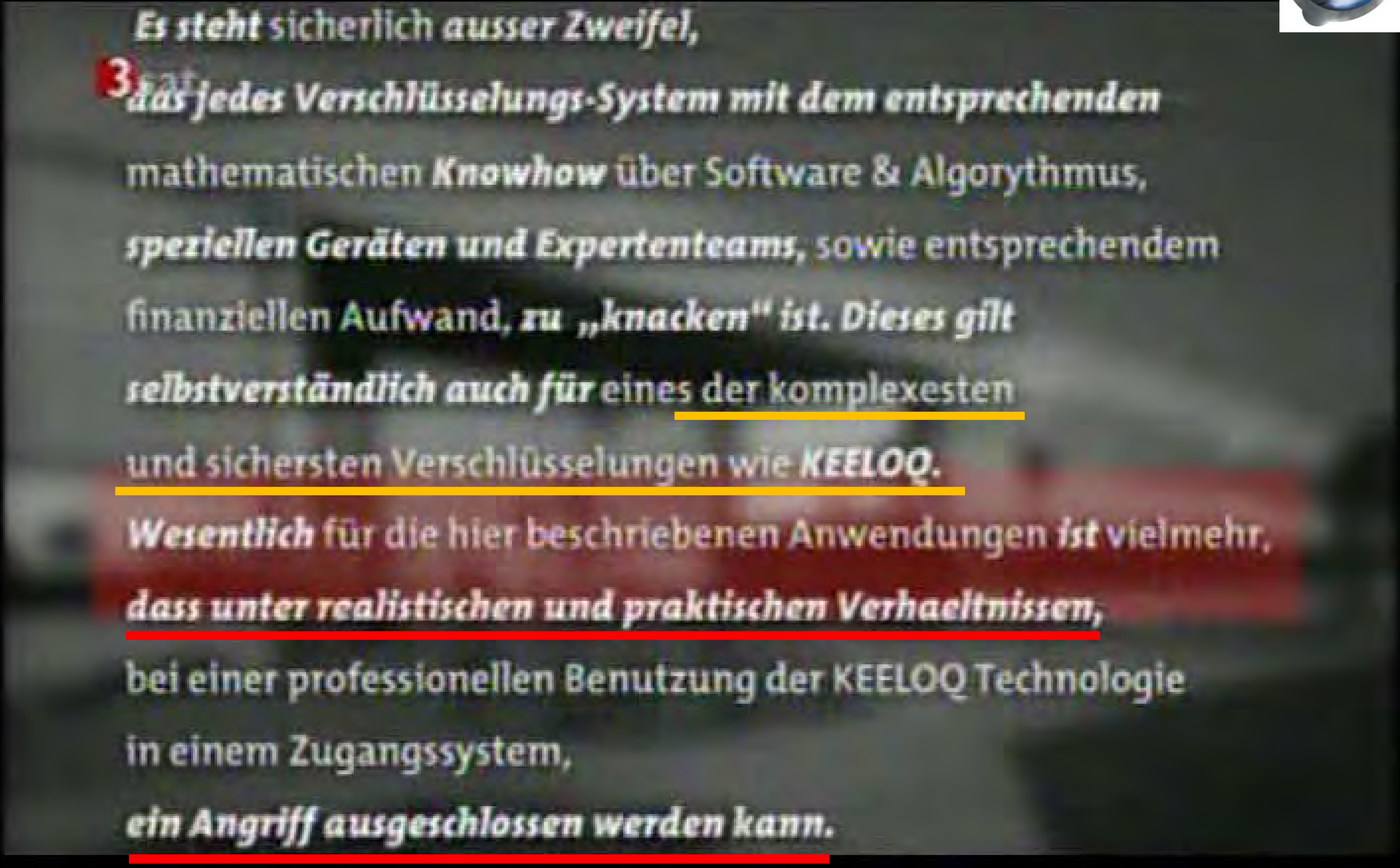
Microchip about KeeLoq:

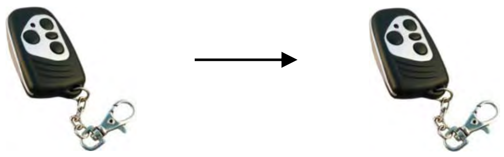


Es steht sicherlich ausser Zweifel,
das jedes Verschlüsselungs-System mit dem entsprechenden
mathematischen Knowhow über Software & Algorythmus,
speziellen Geräten und Expertenteams, sowie entsprechendem
finanziellen Aufwand, zu „knacken" ist. Dieses gilt
selbstverständlich auch für eines der komplexesten
und sichersten Verschlüsselungen wie KEELOQ.
Wesentlich für die hier beschriebenen Anwendungen ist vielmehr,
dass unter realistischen und praktischen Verhaeltnissen,
bei einer professionellen Benutzung der KEELOQ Technologie
in einem Zugangssystem,
ein Angriff ausgeschlossen werden kann.

So what can we do now (1) ?

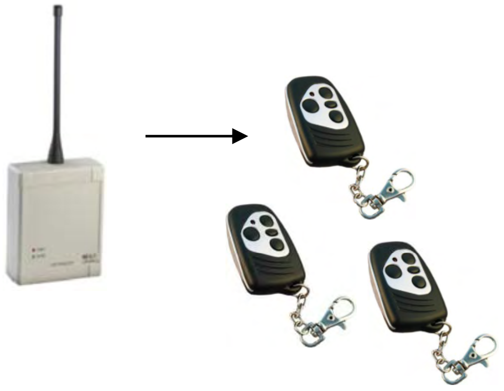
1. If we have access to a remote:

   Recover Device Key and clone the remote



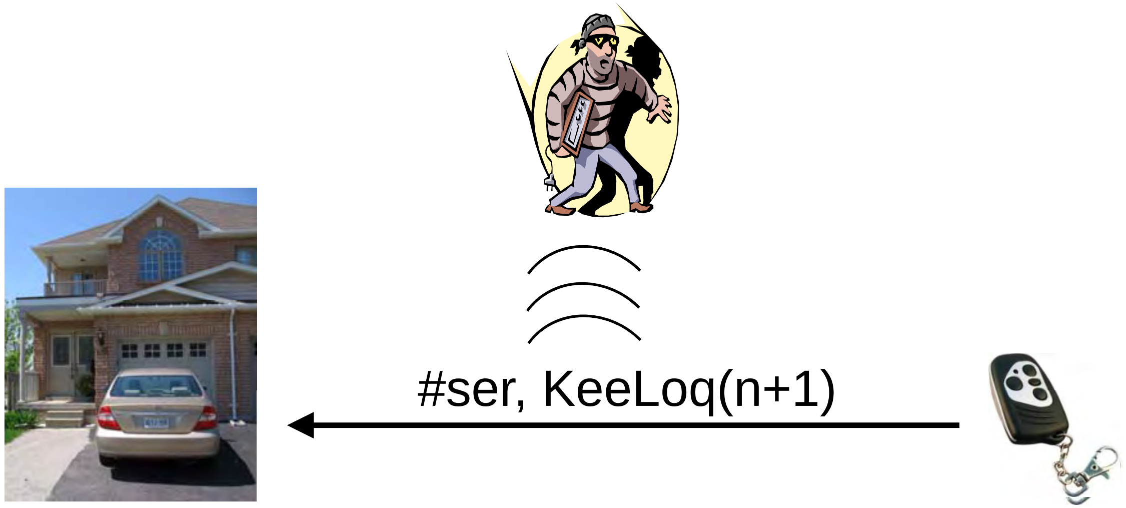
2. If we have access to a receiver:

   Recover Manufacturer Key & generate new remotes



So what can we do now (2) ?

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



www.copacobana.org

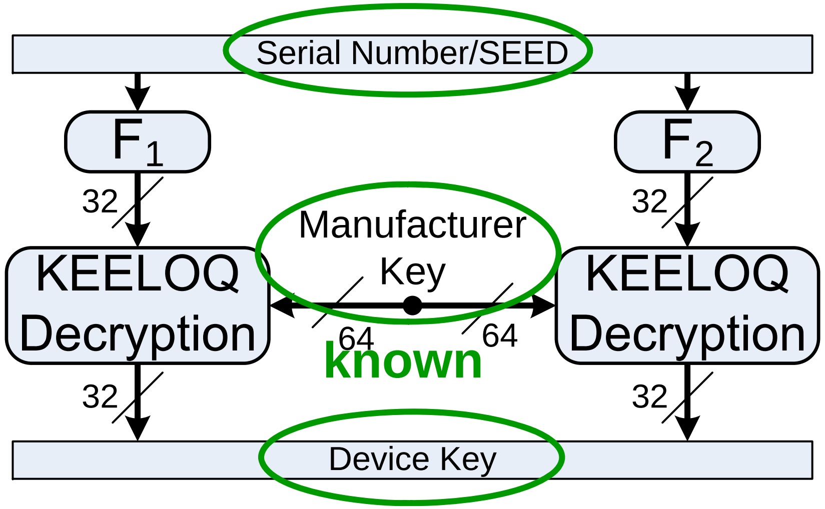
- works for all key derivation schemes
- **instantly** for key derivation from serial number
- otherwise use PC (short seed) or COPACOBANA (long seed)

Details on Eavesdropping Attack

Possessing the Manufacturer Key:

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

known(Serial) or brute-forced(Seed)



…easy.

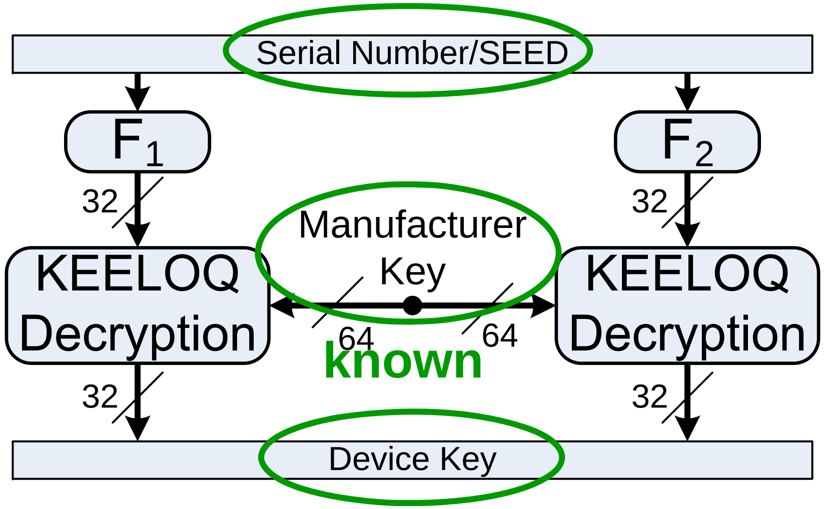
1. Recover Device Key
2. Decrypt Rolling Code → obtain counter etc.
3. Clone the remote control

Details on Eavesdropping Attack

Possessing the Manufacturer Key:

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

known(Serial) or brute-forced(Seed)

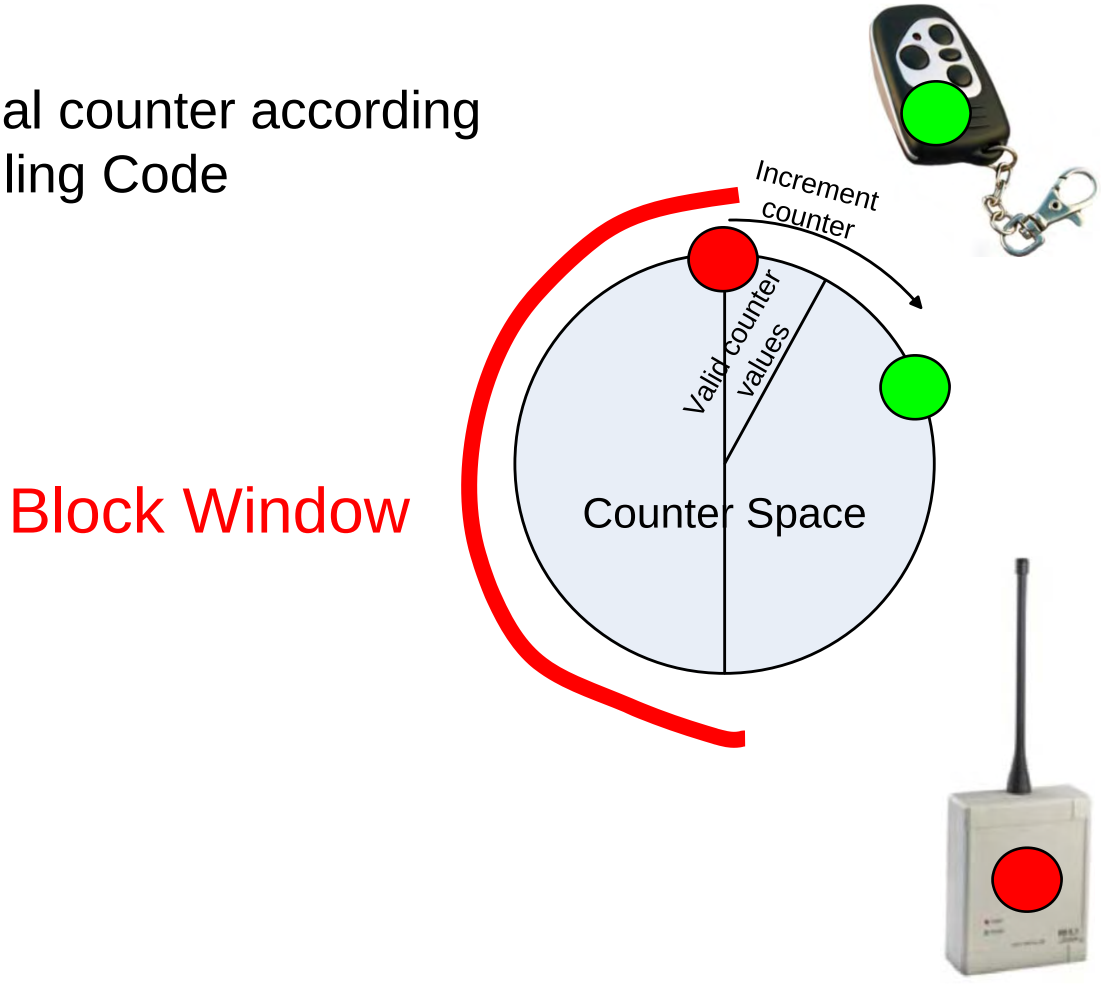


…easy.

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

Taking over a KeeLoq System

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



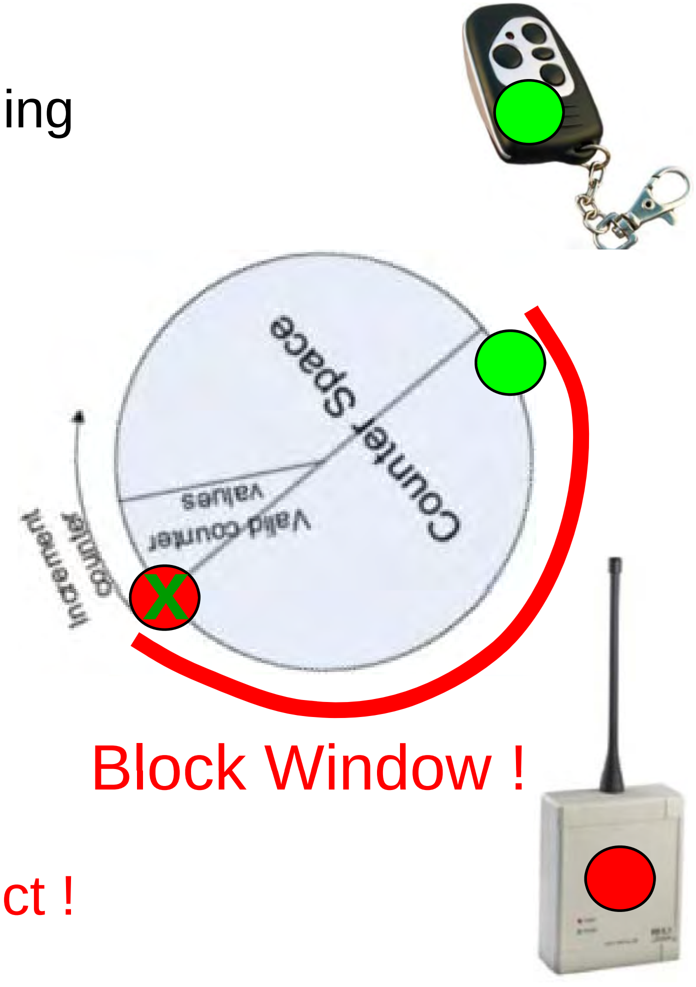
Taking over a KeeLoq System

- 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 !



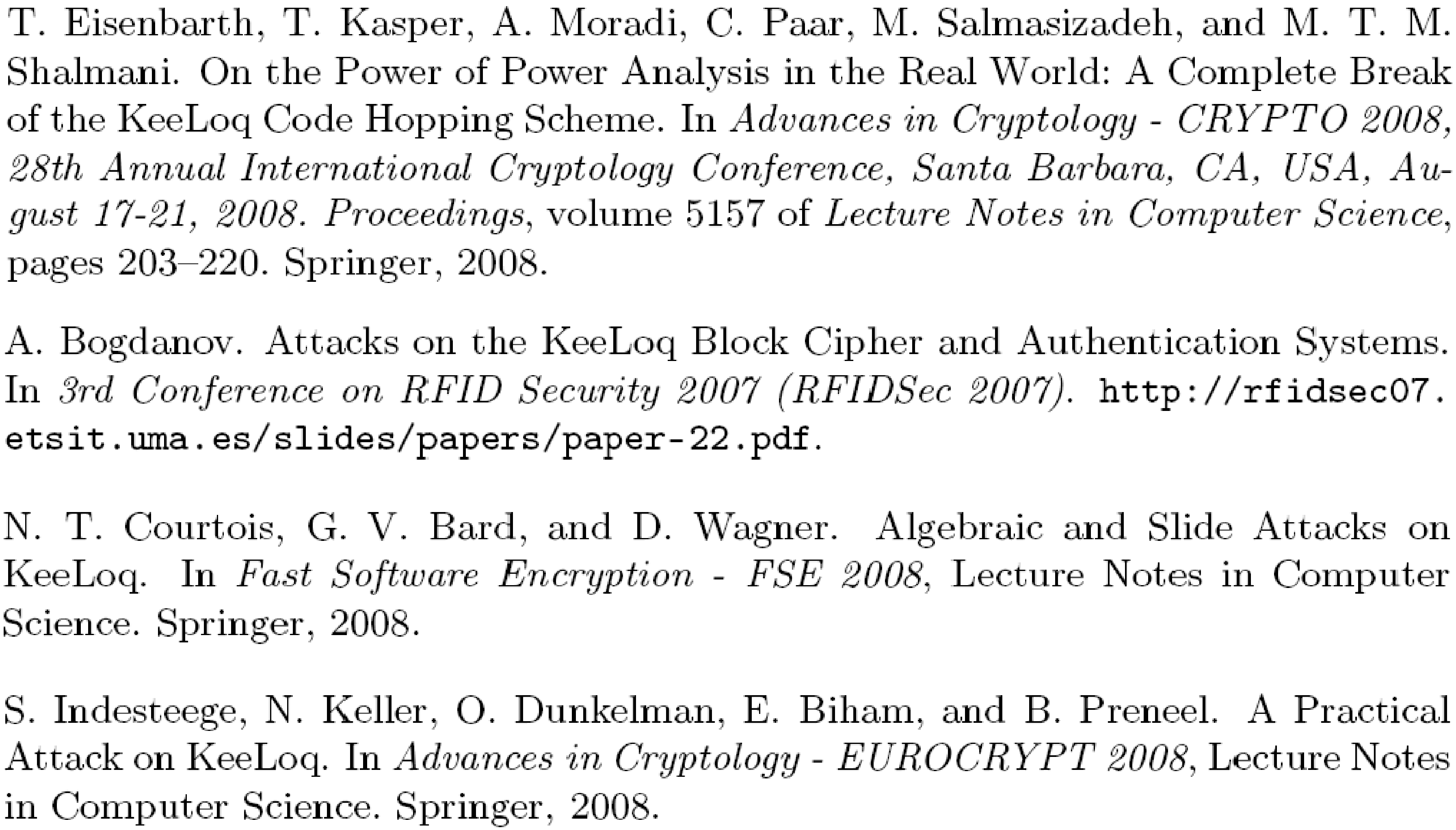
Summary

- “Security only 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, …)
- though SCA is well-known for more than a decade, many embedded / consumer-style applications are still not side-channel resistant

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.

Conferences & Workshops

Workshop on Cryptographic Hardware and Embedded Systems

Lausanne
OLYMPIC CAPITAL

CHES 2009
September 6th – 9th

Switzerland

CHES 2009, September 6-9, Lausanne, Switzerland

Eurocrypt 2009, April 26-30, Cologne, Germany

Thomas Eisenbarth & Timo Kasper

contact: *keeloq@crypto.rub.de*

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

A Naming Tale (2005)

possible abbrevations for„Cost-optimized Parallel Code-Breaker“

CPCB?

COPCOB?

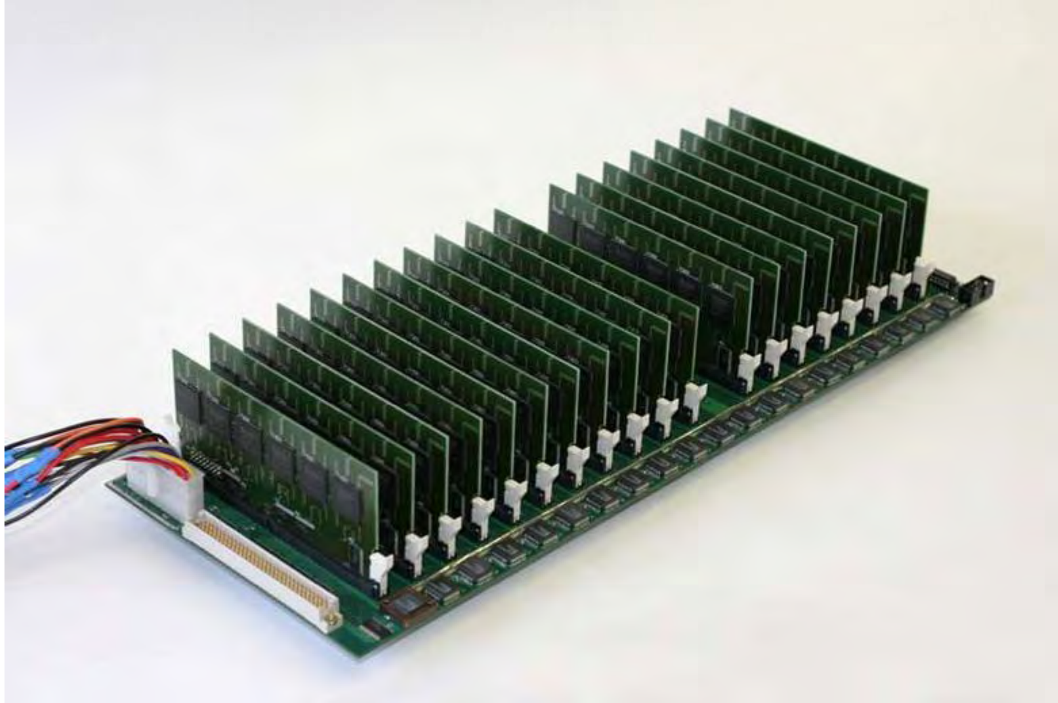
COPCOBRA?

COOPACOB?

COPACOBRA?

...

► **COPACOBANA**

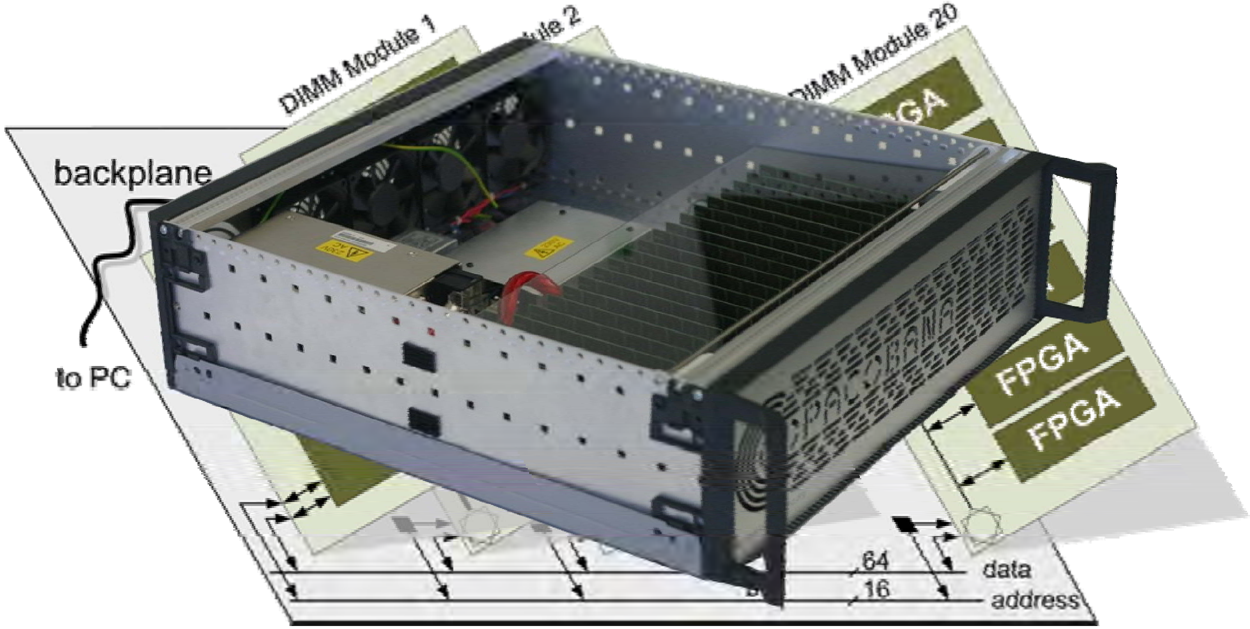


A Naming Tale

… Easy to remember: Copacabana…

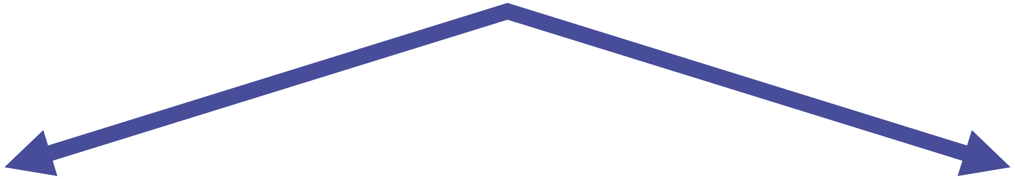
COPACOBANA

- Cost-Optimized PArallel COde Breaker
- FPGA-based reconfigurable machine for cryptanalysis
- Parallel architecture built out of 120 Xilinx Spartan3 FPGAs
- Modular design:
  - Backplane with FPGA modules (each with 6 low-cost FPGAs)
  - Controller card with USB interface or TCP/IP Interface

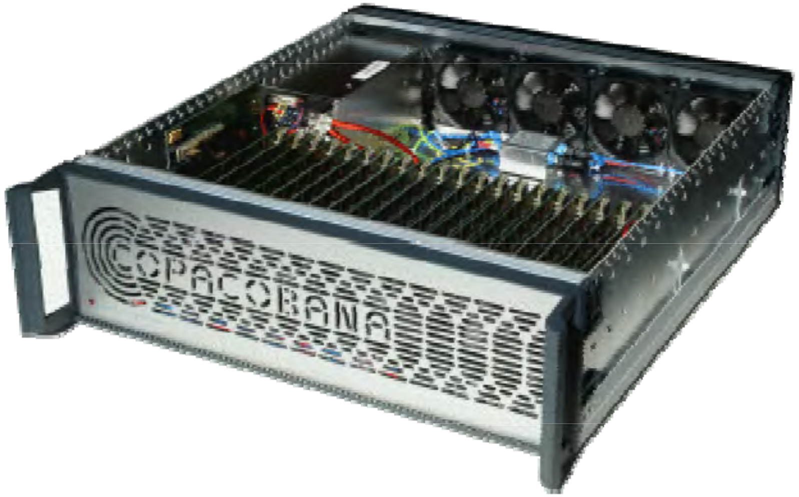


To break DES in 6.4 days in average

- You need



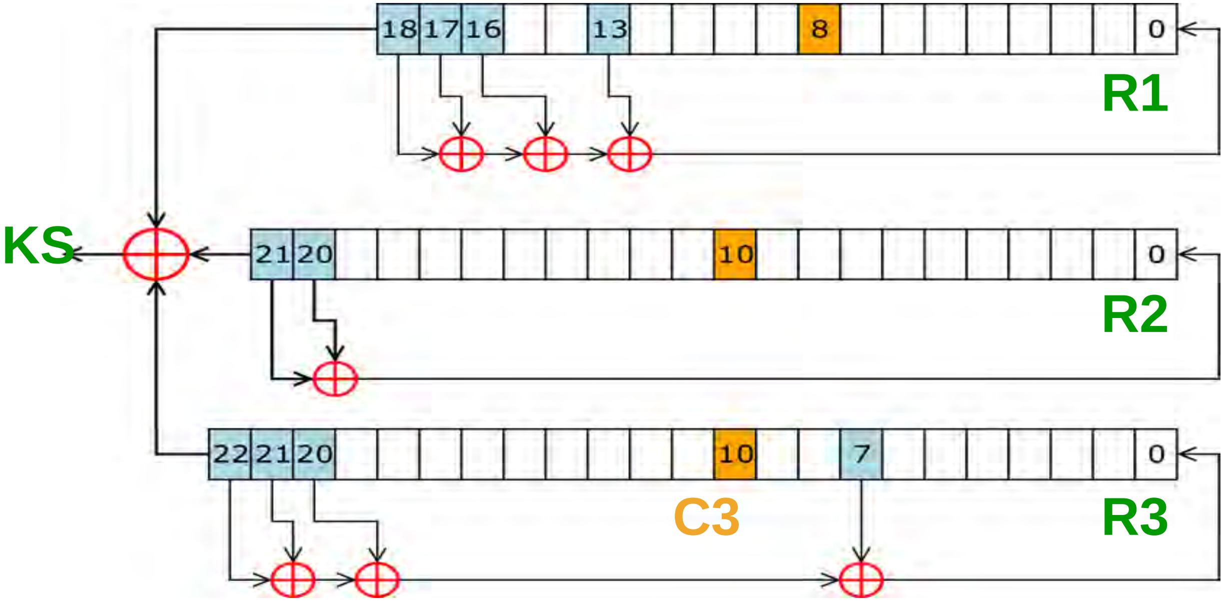
32,640 PCs or 1 COPACOBANA



Breaking the A5/1

- Guess complete content of **R1**, **R2**
- Derive content of **R3** step-by-step:
  a. Derive **MSB** of **R3** from **R1**, **R2**, and known **KS**
  b. Guess **C3** (clocking bit of R3)

  until **R3** is completely determined.
- Continue clocking A5/1 & compare generated **KS** against known **KS**
- If **64** bits of generated **KS** match, then **CANDIDATE FOUND**



Break electronic passports

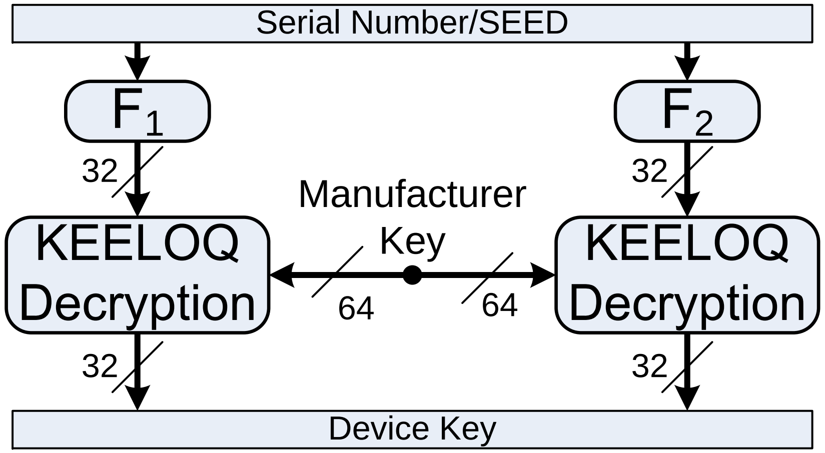
- weak keys in
  Basic Access Control (BAC)

- possible real-time attack
  with COPACOBANA

… steal identities, track people, trigger alarms, …

Break KeeLoq with COPACOBANA

After extracting the Manufacturer Key (needs to be done only once)
if SEED is used → brute force SEED space



Serial Number/SEED

KEELOQ Decryption

KEELOQ Decryption

Device Key

- 110 million keys / second verified in 1 FPGA Spartan 3-1000
- **32 bit seed:** **39 seconds / 1 FPGA**
- **48 bit seed:** **5.9 hours / 1 COPACOBANA**
- **60 bit seed:** **101 days / 10 COPACOBANAs**

→ 60 bit resists brute force - but we haven‘t seen it used