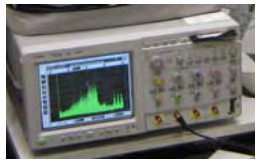
Performing the Side-Channel Attack



Analyze cipher

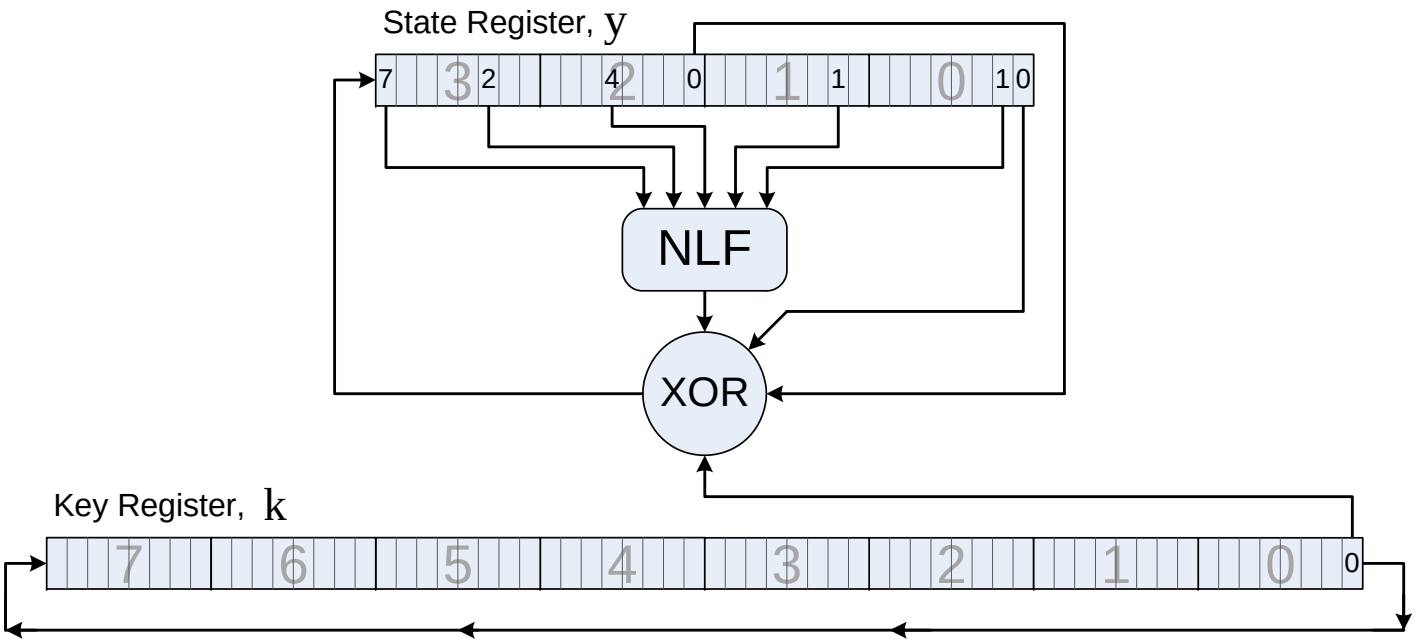
Measurements

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

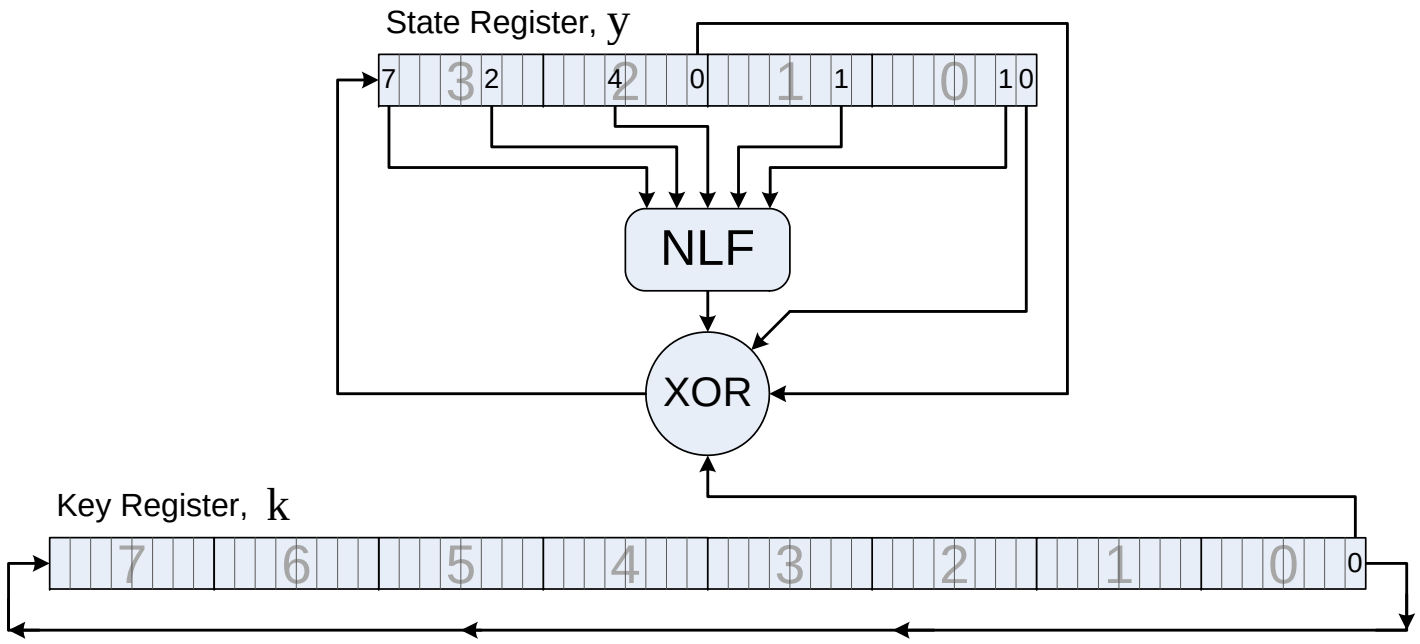
KeeLoq – Algorithm



- 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

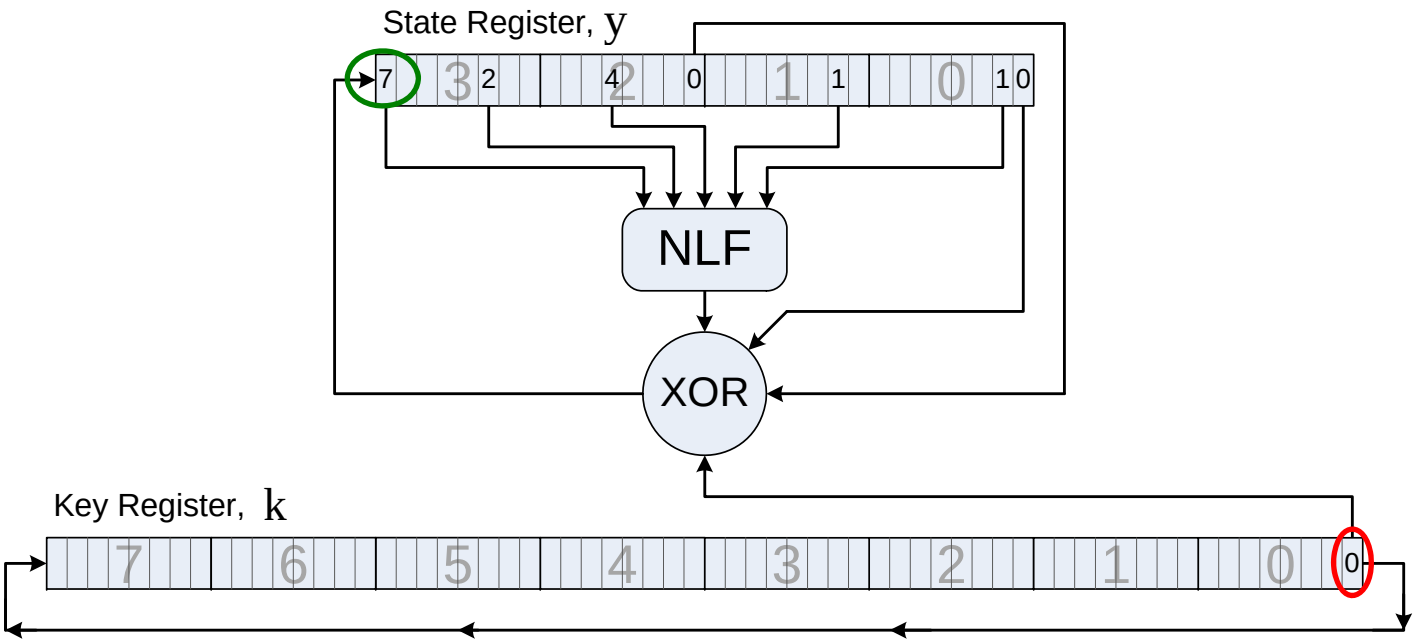


Power Consumption:

- 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 the State Register

KeeLoq – Attack

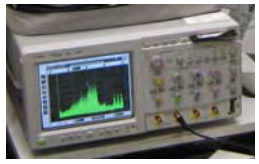


$$y_{31}^{(i+1)} = k_0^{(i)} \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus \mathrm{NLF}\left(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}\right)$$

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

→ Analyzing variations of the state will reveal the secret key

Performing the Side-Channel Attack



Analyze cipher

Measurements

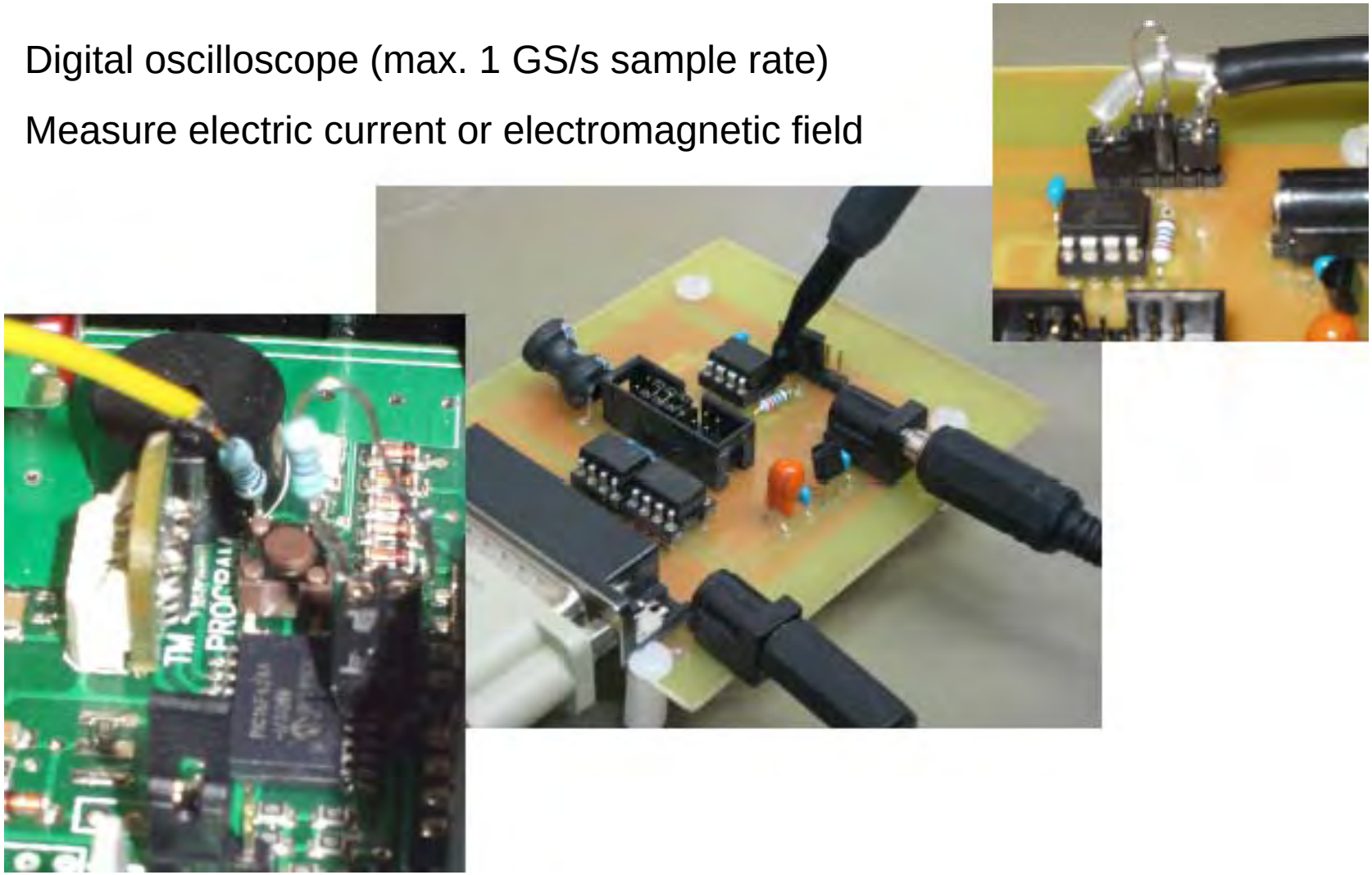
Post Processing

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

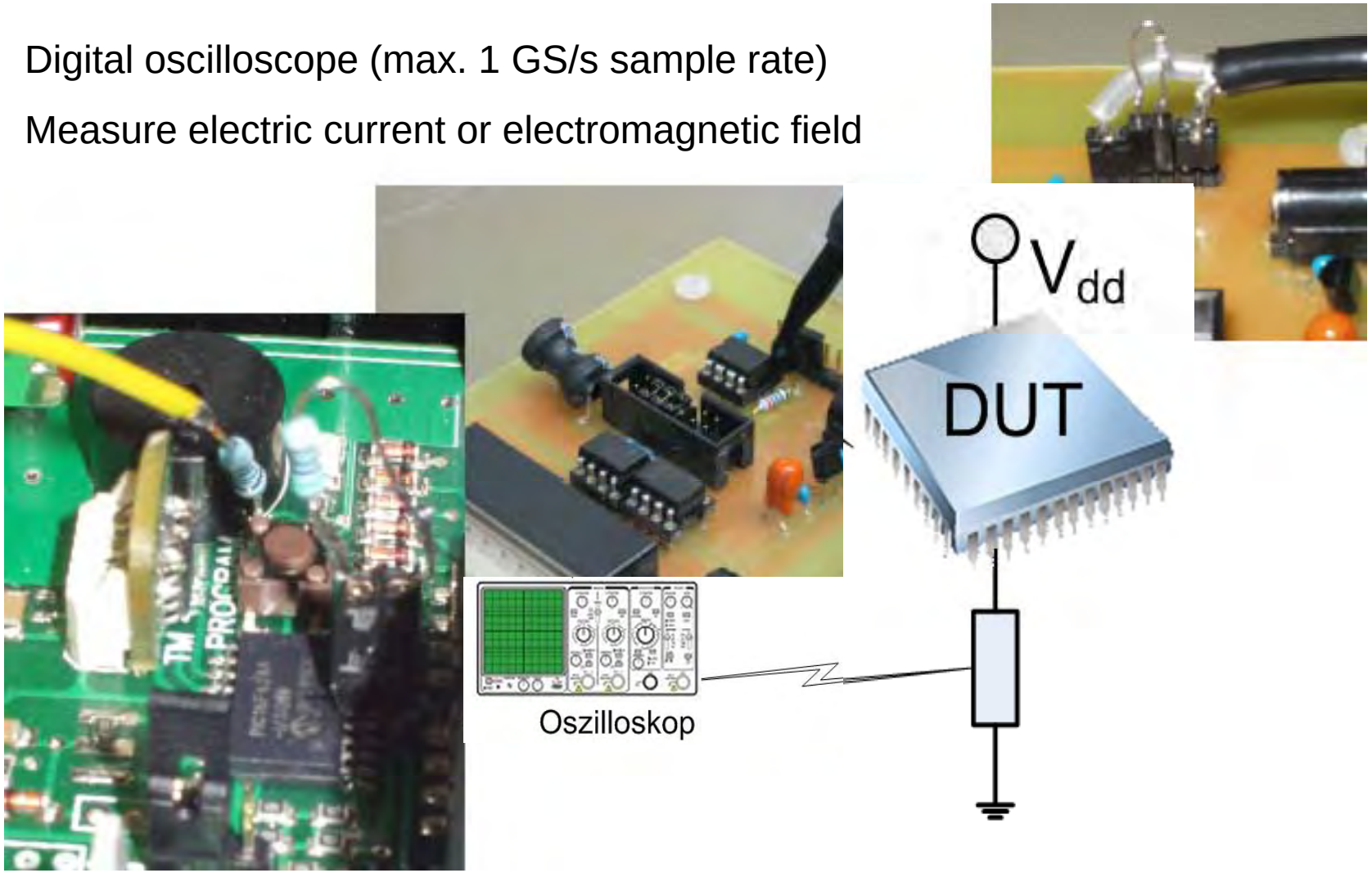
Measuring the Power Consumption

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

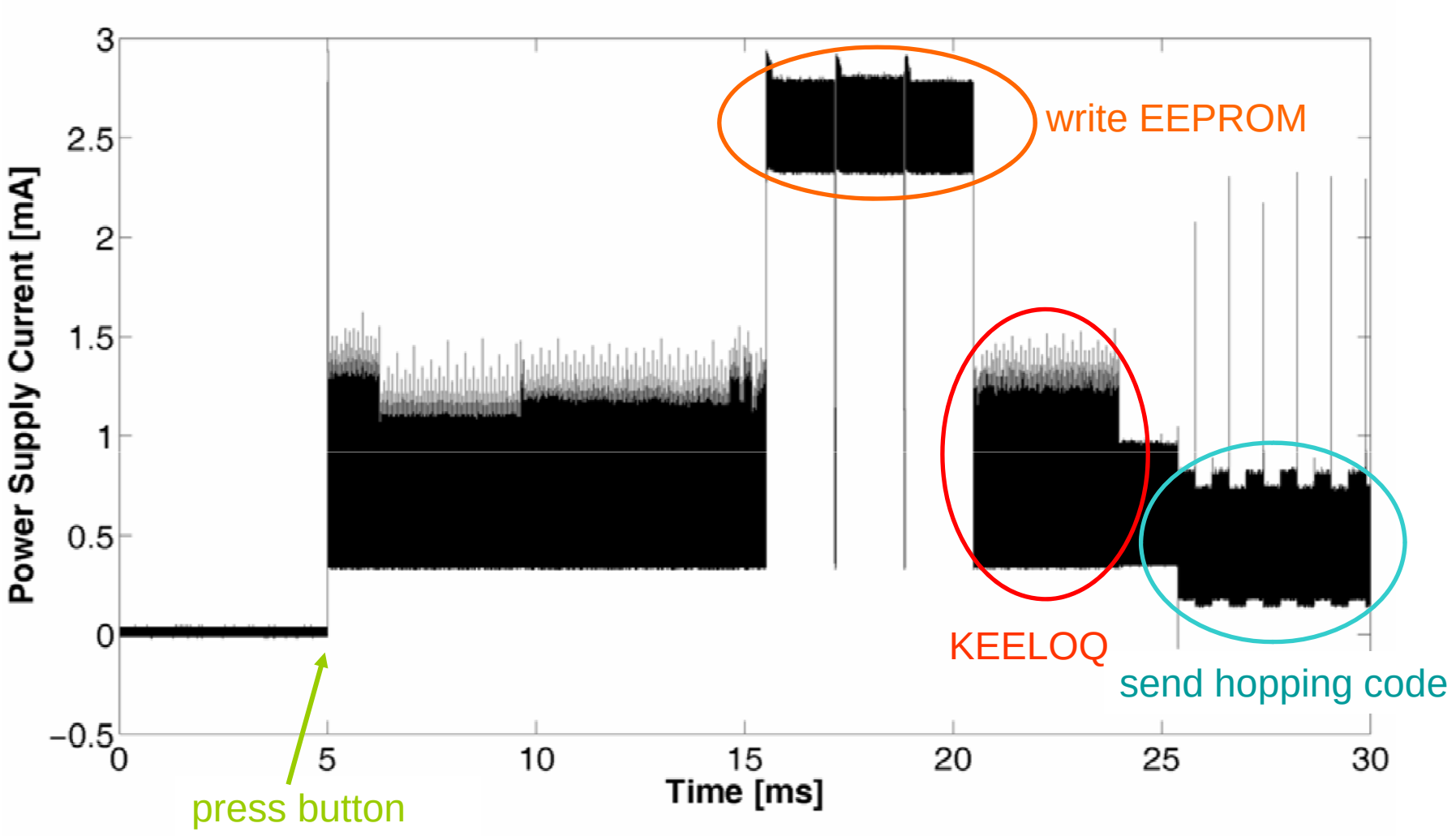


Measuring the Power Consumption

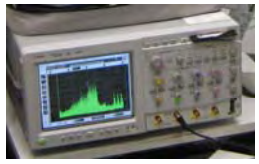
- Digital oscilloscope (max. 1 GS/s sample rate)
- Measure electric current or electromagnetic field



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

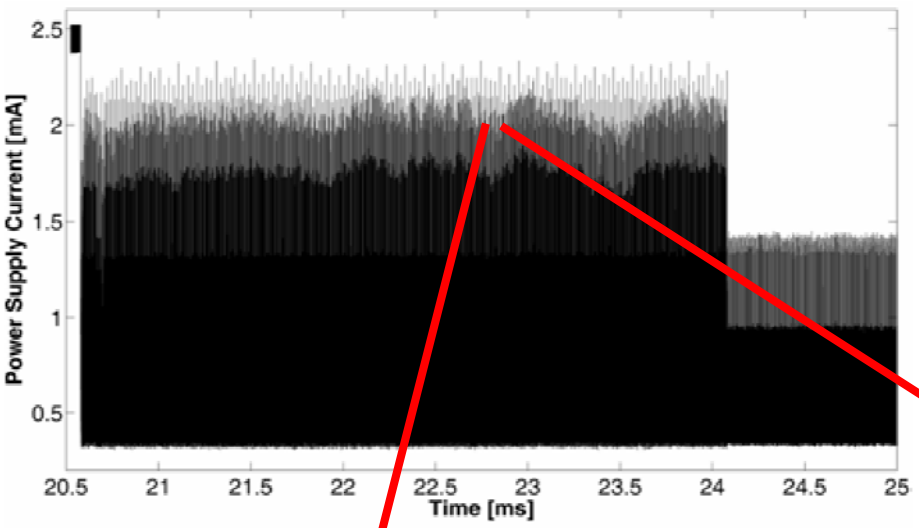


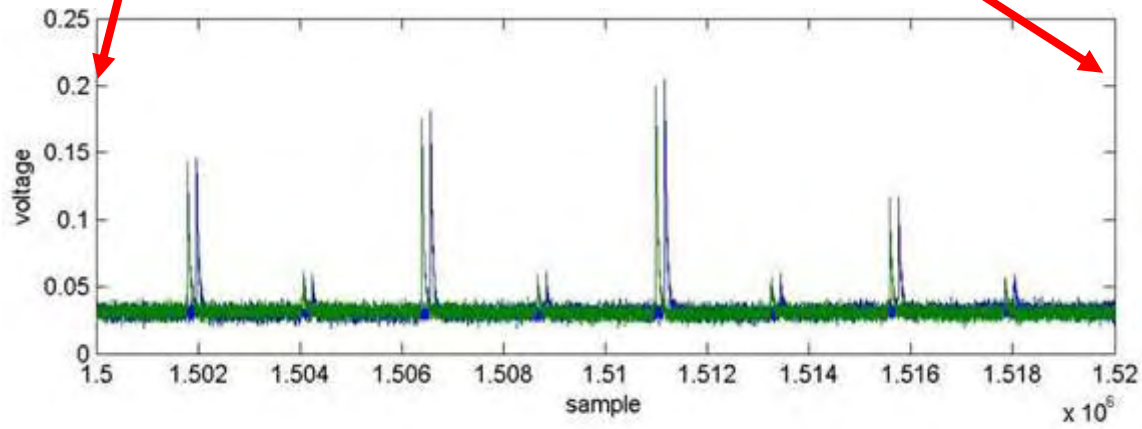
Performing the Side-Channel Attack



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



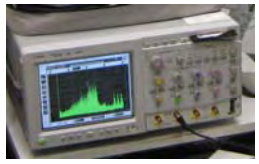


Main problems:

- 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



Analyze cipher

1. Find a suited predictable intermediate value in the cipher

Measurements

2. Perform power measurements

Post Processing

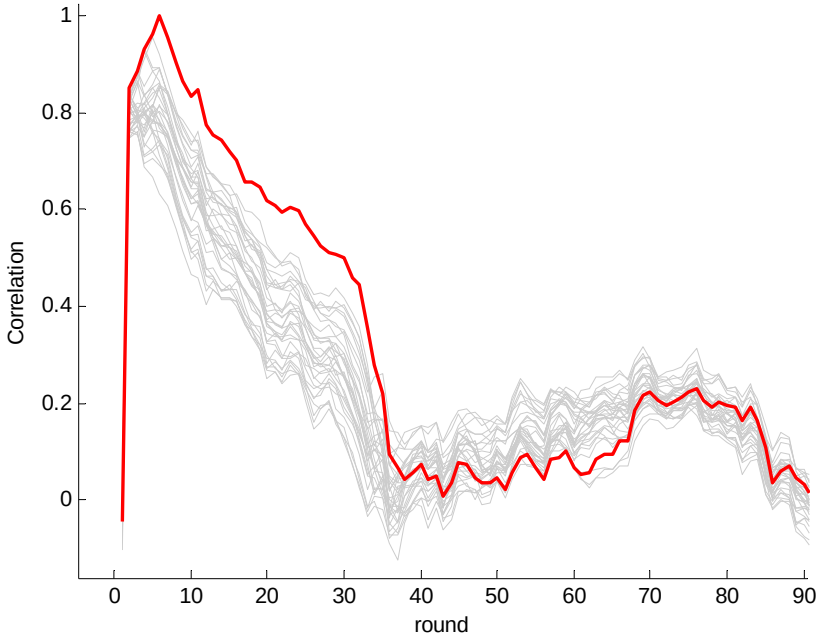
3. Align and reduce size of acquired data

Key Recovery

4. Correlate measurements with model

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
- Let the best-matching key candidates “survive“

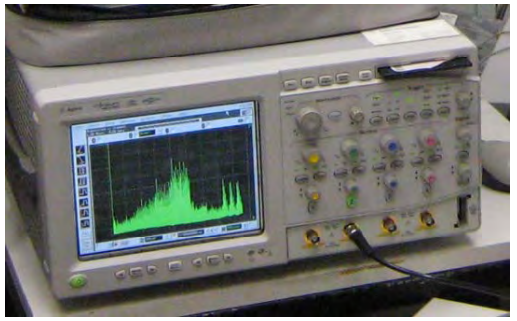


$$r\left(I_i(t), D(X_i, K_h)\right) = \frac{\sum_{i=1}^{M} I_i(t) \cdot D(X_i, K_h)}{\sqrt{\sum_{i=1}^{M}\left(I_i(t) - \overline{I_i(t)}\right)^2 \cdot \sum_{i=1}^{M}\left(D(X_i, K_h) - \overline{D(X_i, K_h)}\right)^2}} - \frac{\frac{1}{M} \cdot \sum_{i=1}^{M} I_i(t) \cdot \sum_{i=1}^{M} D(X_i, K_h)}{\sqrt{\sum_{i=1}^{M}\left(I_i(t)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

DPA Workshop @ 25C3

Horst-Görtz Institut für IT Sicherheit

Learn to perform your own DPA !!!



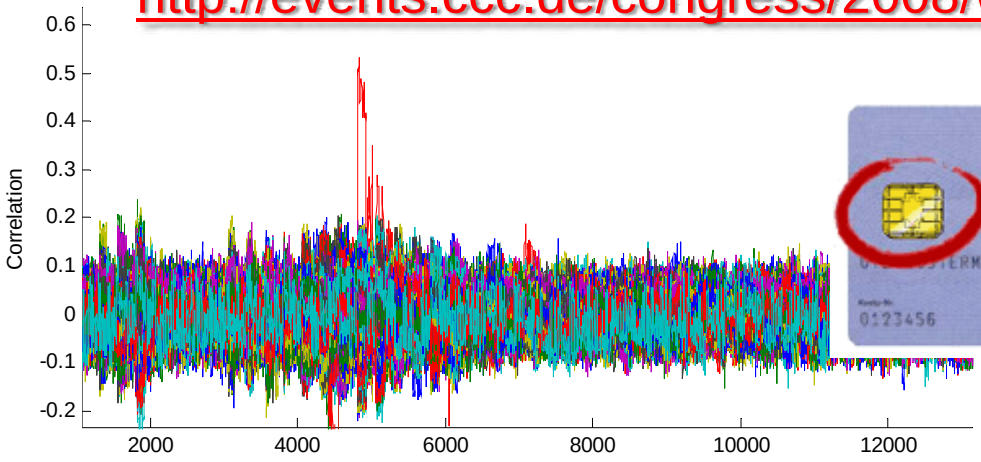
Recover Keys from:

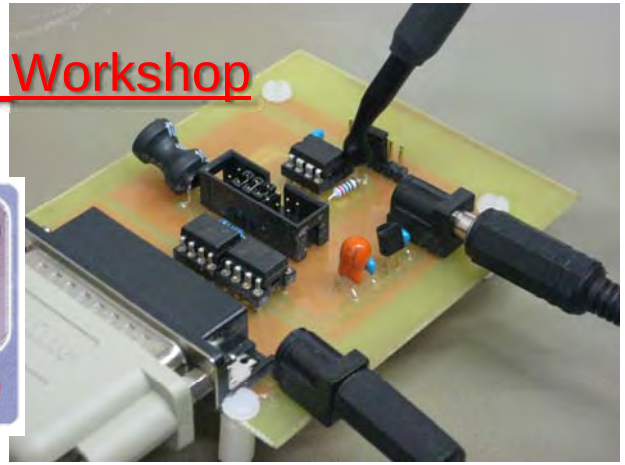
– KeeLoq Transmitter IC (HCS Chip)

– Smart Card featuring an AES Implementation

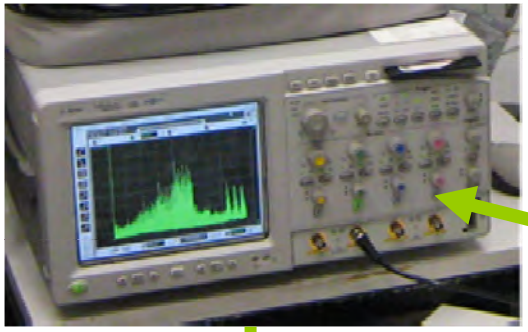
Further information:

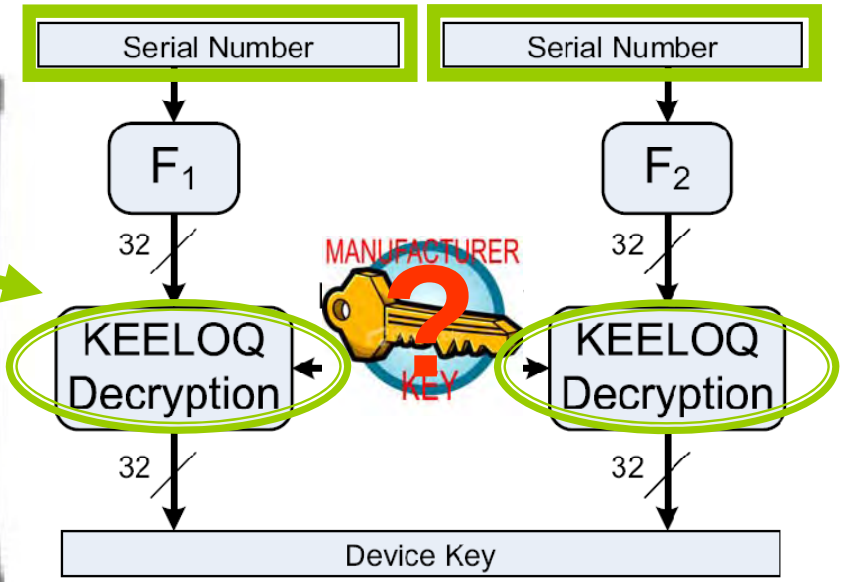
http://events.ccc.de/congress/2008/wiki/DPA_Workshop





Power Analysis of the Receiver



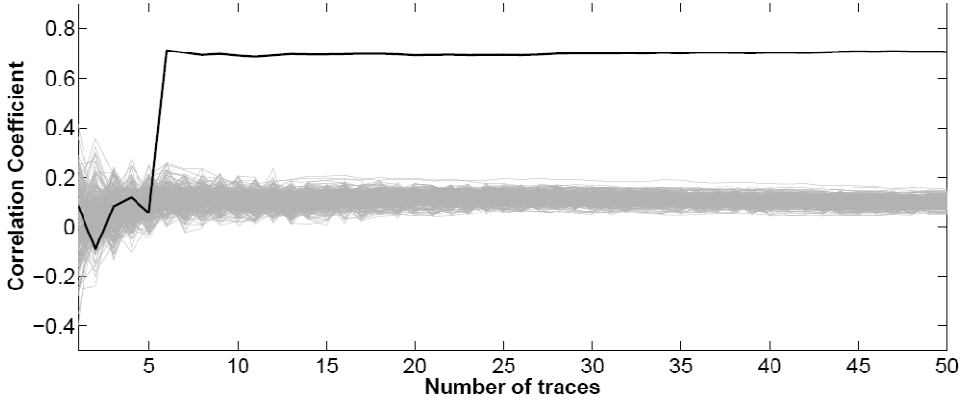


secret key of manufacturer!

Side-Channel Attack Results for KeeLoq

A) Hardware implementation (“car key“)

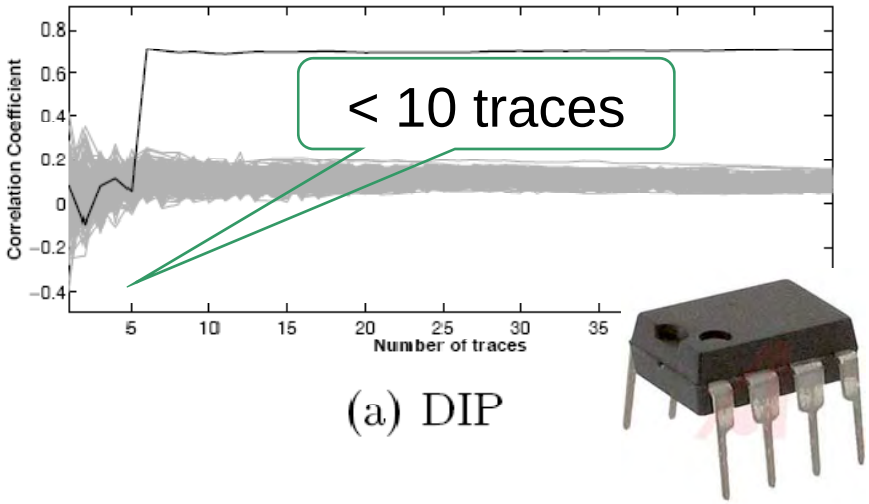
- Total attack time (for known device family):
  5-30 traces, ≈ minutes



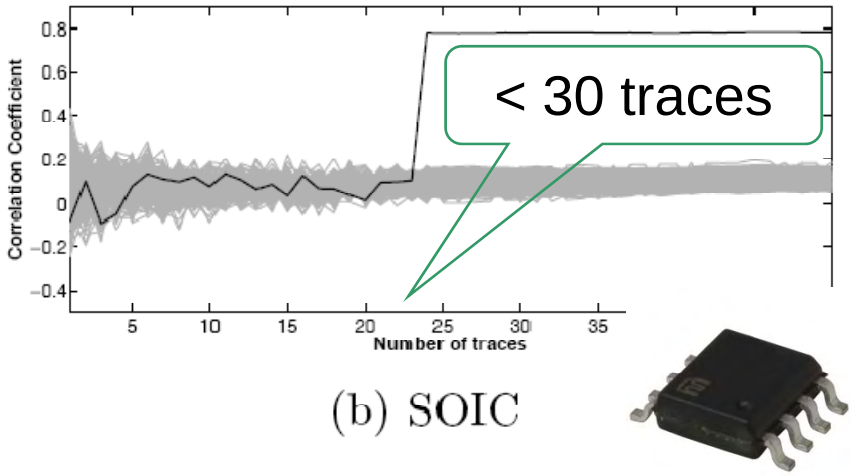
B) Software implementation (“car door“)

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

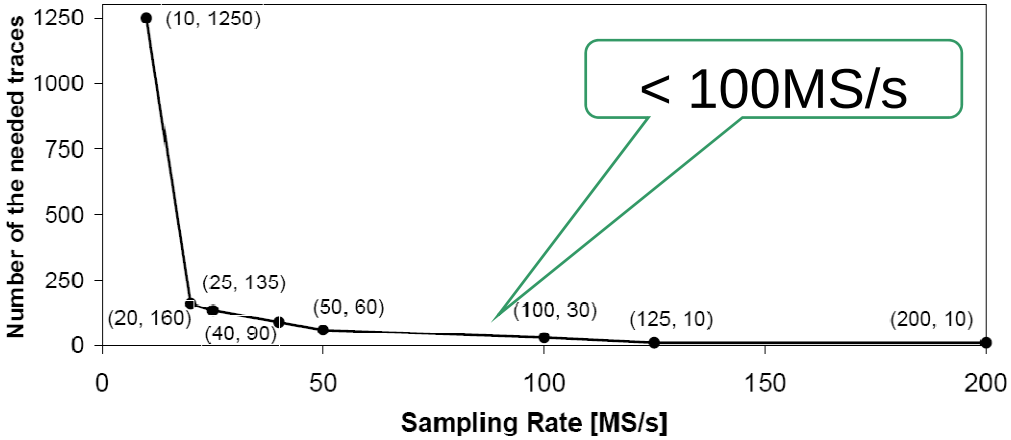
Comparison of Packages & Sample Rates



(a) DIP



(b) SOIC



No expensive equipment needed for key recovery !