COSIC
CRYPTOGRAPHY & CYBER SECURITY

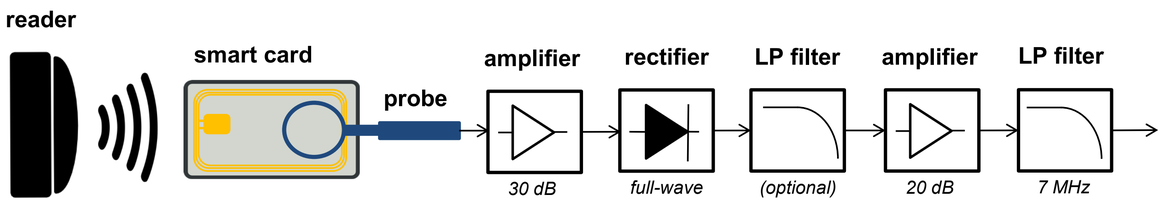
Comparison of two Setups for Contacless Power Measurement for Side-Channel Analysis

Arthur Beckers, Benedikt Gierlichs, Josep Balasch and Ingrid Verbauwhede

Aim

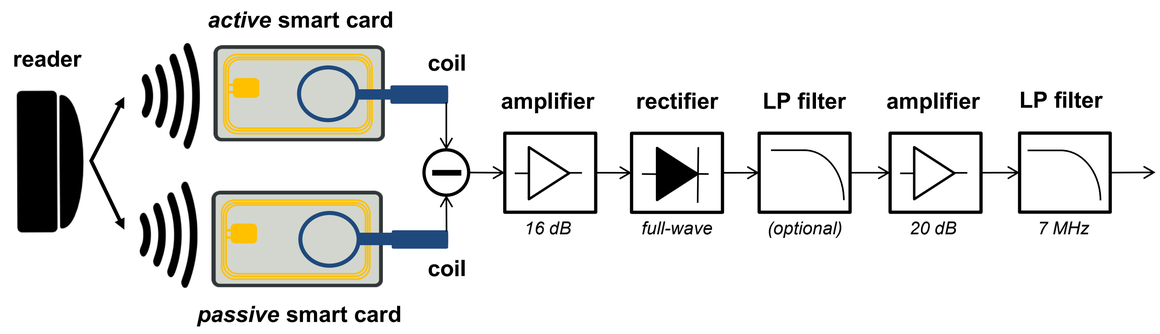
- Goal: quality evaluation of antenna setup to measure instantaneous power consumption of contactless smartcards
- Comparison of two measurement setups:
  - * Traditional single antenna setup
  - * Novel balanced setup
- Main challenge is removing the carrier field from the side channel measurement

1) Single Antenna setup



- Reader : Microprocess smart card emulator
- Probe : wide band EM probe (Langer LF-R 400)
- Amplifier: Langer LNA 30 dB
- Analog processing: Envelope detector + 2MHz and 7MHz low pass filter

2) Balanced Setup

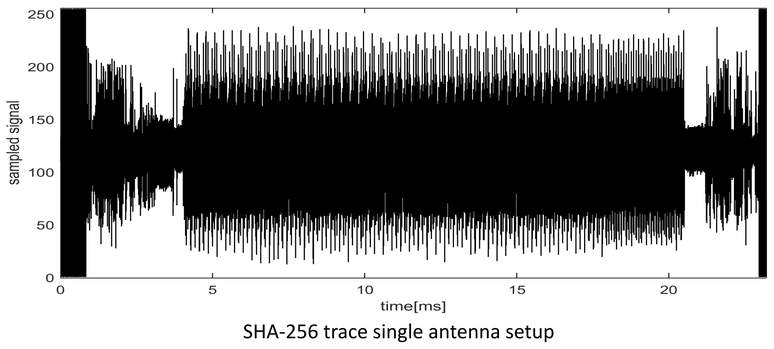


- Probe : two ferrite cores which allow for differential measurement of two identical smartcards.
- The rest of the components are identical to those used in the single antenna setup

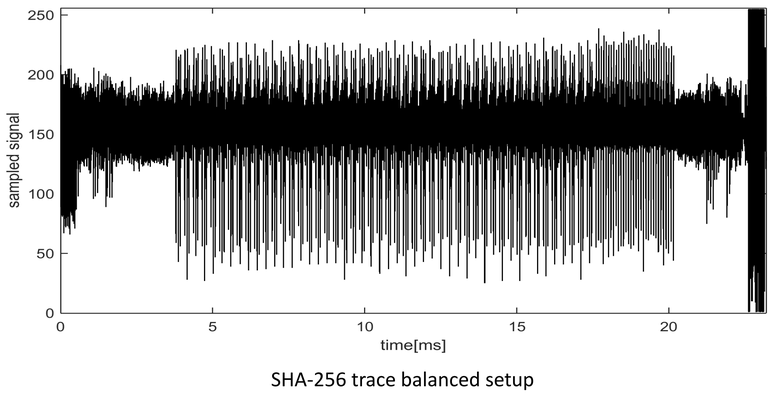
Target

Contactless smartcard: BasicCard model ZC7.5 rev B

- Compliant with ISO 14443
- Uses a 13.56 MHz carrier field
- Contains 8 bit microcontroller
- Target operation is a software implementation of SHA-256



SHA-256 trace single antenna setup

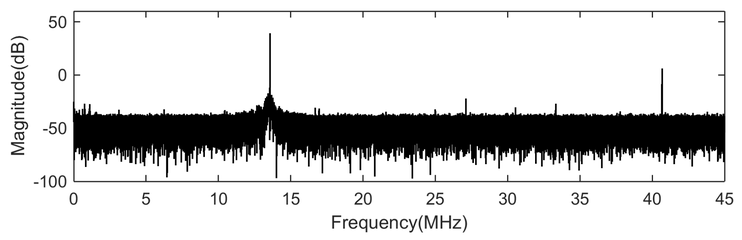


SHA-256 trace balanced setup

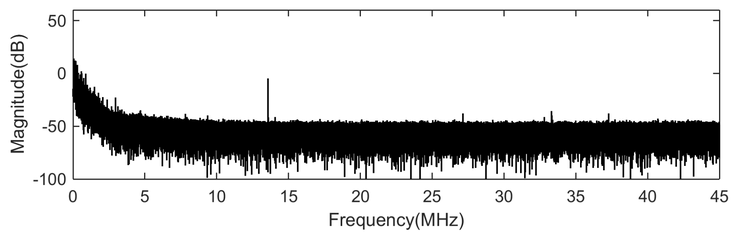
FFT

a) FFT single antenna setup without analog postprocessing
b) FFT single antenna setup with analog post-processing
c) FFT balanced setup with analog post-processing

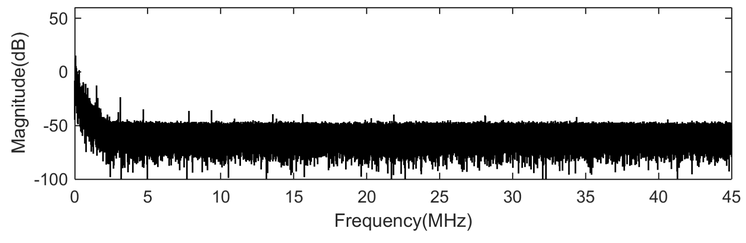
a)



b)



c)



Measurement quality assessment

Signal to noise ratio (SNR) as metric for measurement quality

- * Signal = power consumption related to internal state SHA-256
- * Noise = all the rest (mainly carrier field)

$$SNR = \frac{Var(\{\mu_i\})}{Mean(\{\sigma_i^2\})}$$

SNR results SHA-256

- SHA-256's internal state consists of 8 32 bit values (a, b, … , f, g)
- Target an 8 bit chunk of one of the 32 bit state values
- $a_{j,k}$ = chunk k of state value a after round j

Target variable	SNR	SNR
$HW(a_{0,1} \oplus a_{1,1})$	0.1683	0.1604
$HW(a_{0,2} \oplus a_{1,2})$	0.2723	0.2307
$HW(a_{0,3} \oplus a_{1,3})$	0.1456	0.1432
$HW(a_{0,4} \oplus a_{1,4})$	0.1661	0.1415
$HW(a_{1,1} \oplus a_{2,1})$	0.1174	0.0908
$HW(a_{1,2} \oplus a_{2,2})$	0.1276	0.0969
$HW(a_{1,3} \oplus a_{2,3})$	0.1306	0.1128
$HW(a_{1,4} \oplus a_{2,4})$	0.1336	0.0934

Conclusion

- Single antenna setup performs slightly better than balanced setup
- Results depend strongly on target and analog post-processing components
- More experiments are needed to make a definitive conclusion

FUNDING

KU LEUVEN erc