

brightsight®



your
partner
in security
approval



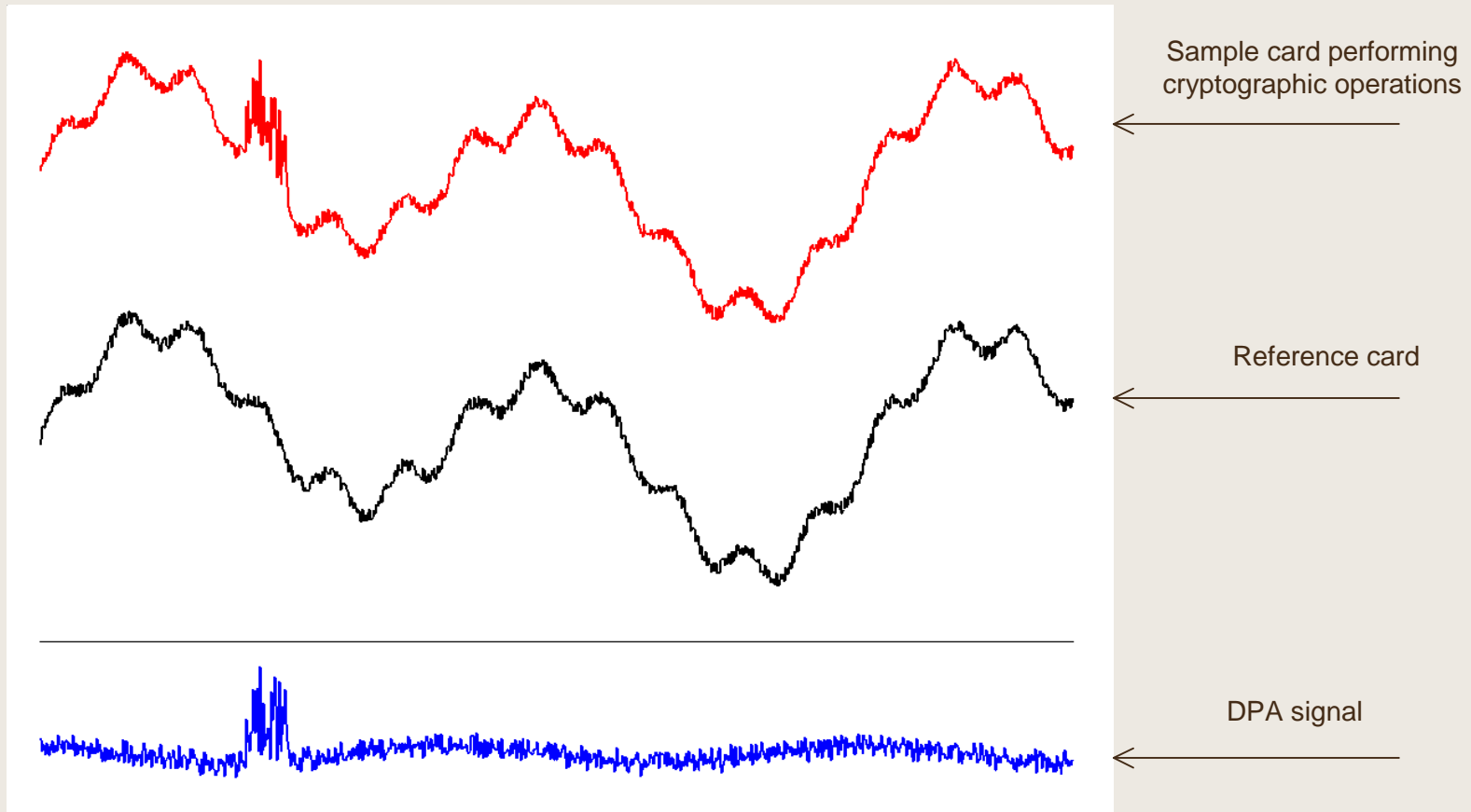
Monique Bakker
+ 31 15 269 2502
bakker@brightsight.com
www.brightsight.com

**Contact-less DPA on smart
cards must be considered
under vulnerability
assessment (AVA_VAN)**

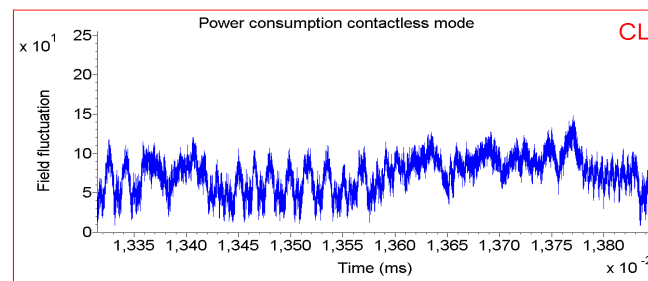
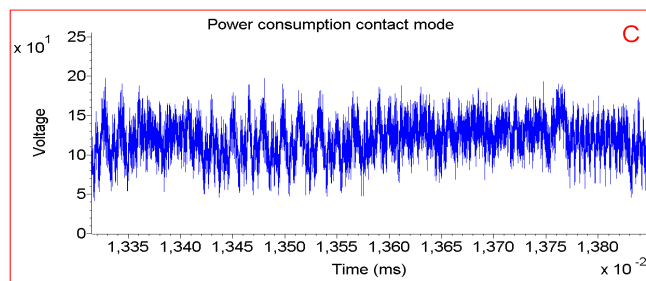
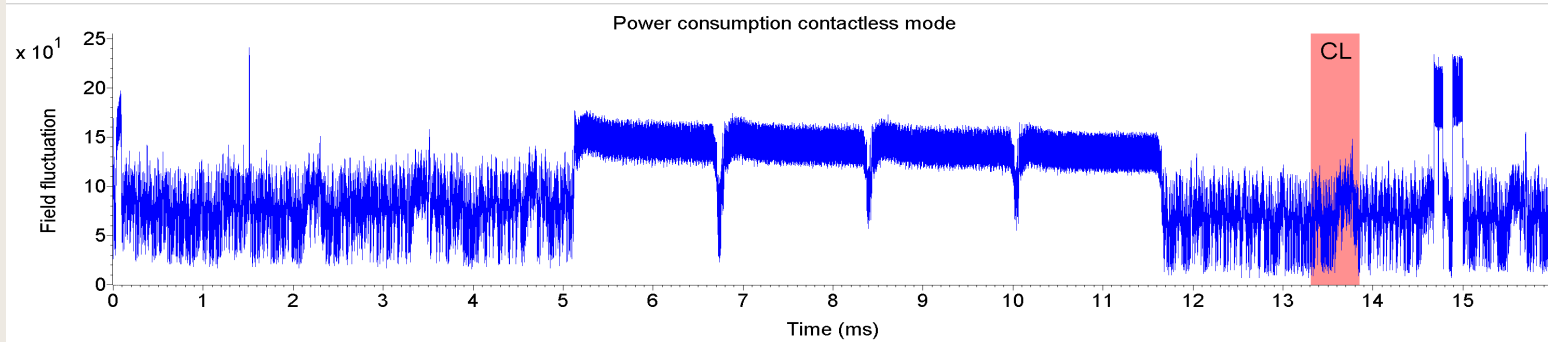
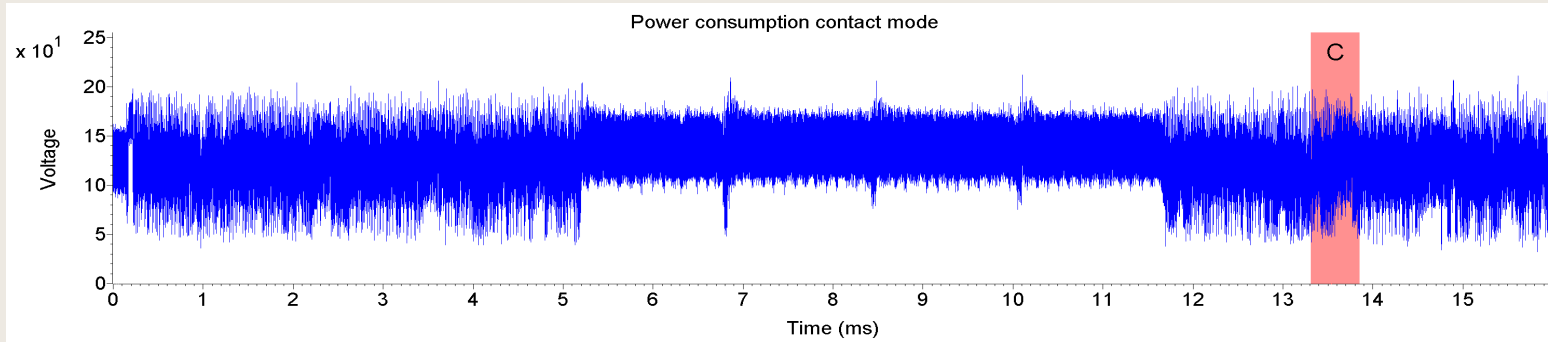
Presentation content

- Attack characteristic
- Tools used
- Practical results
- Attack rating
- Considerations in AVA_VAN
- Conclusion

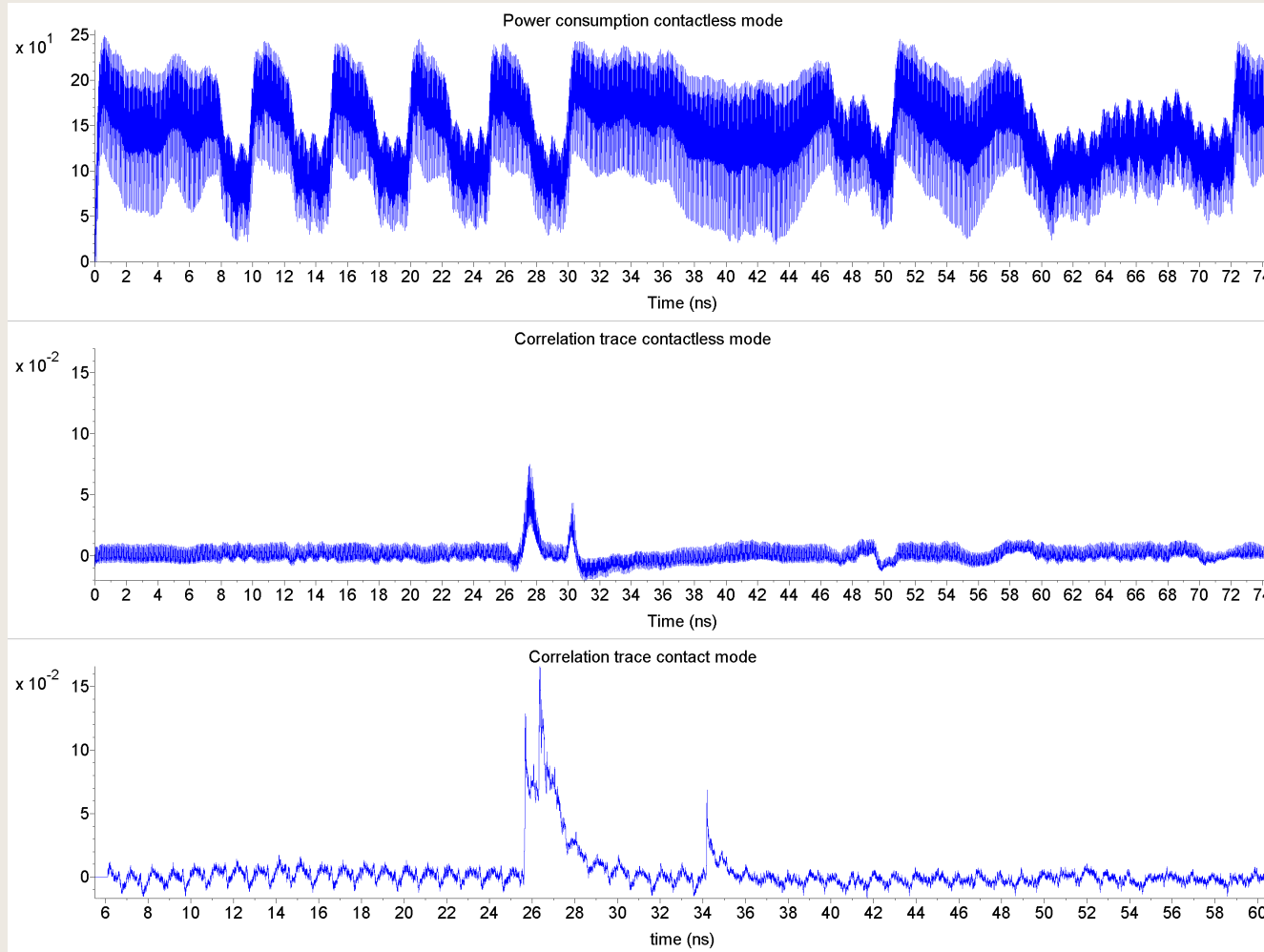
Measurement approach



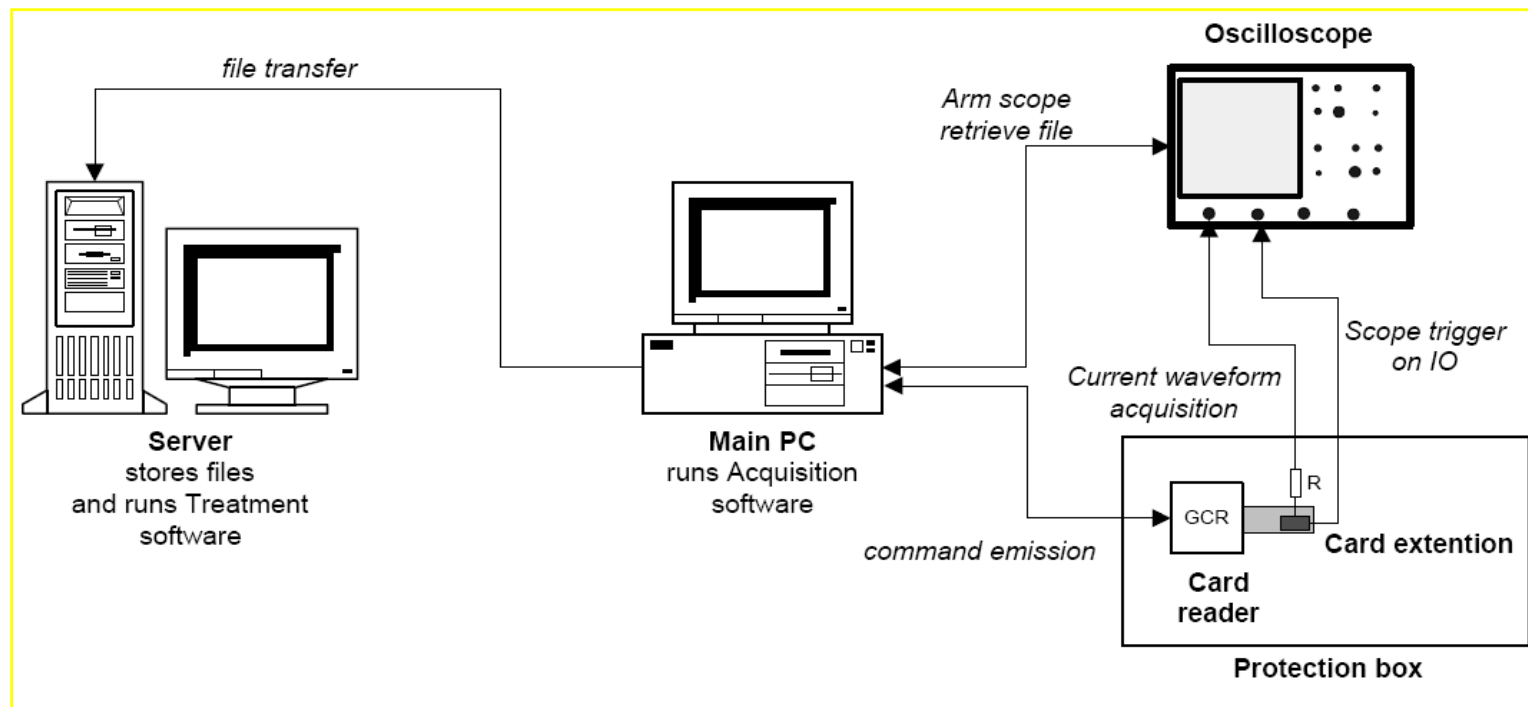
Similarity of measured signal



Correlation traces

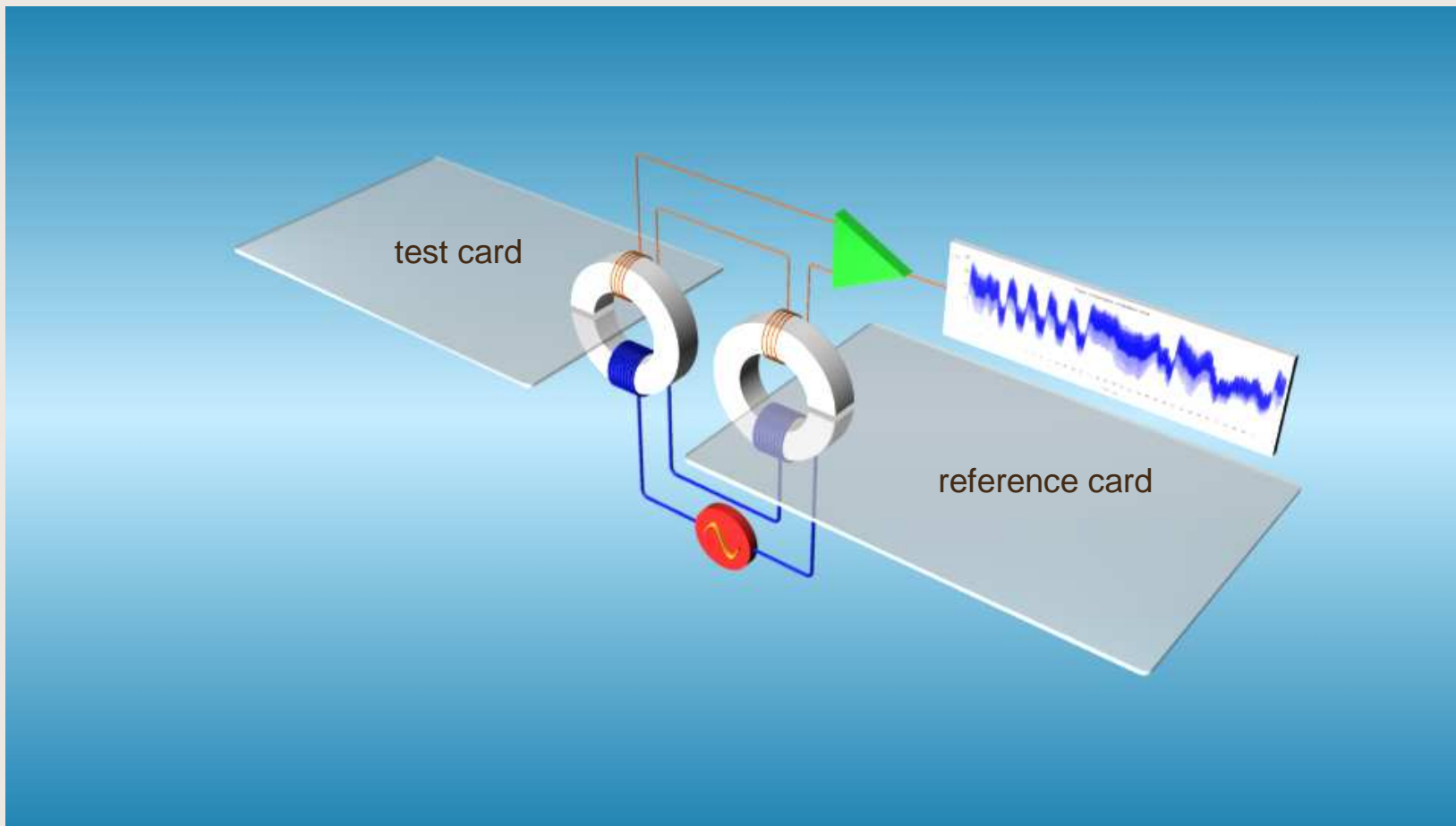


Complete set-up for contact DPA

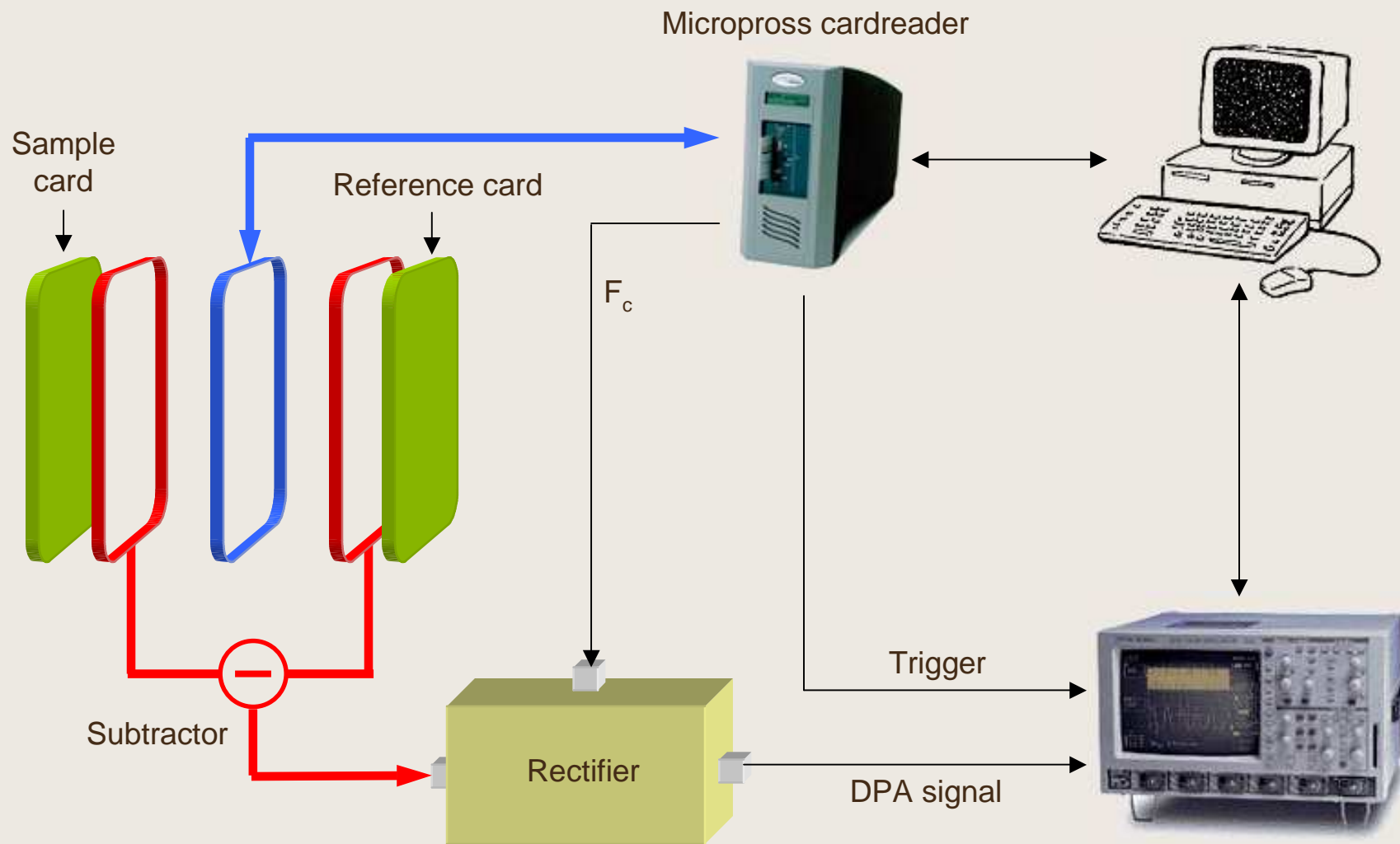


This picture is copied from 'JIL Attack Methods for Smartcards and Similar Devices'

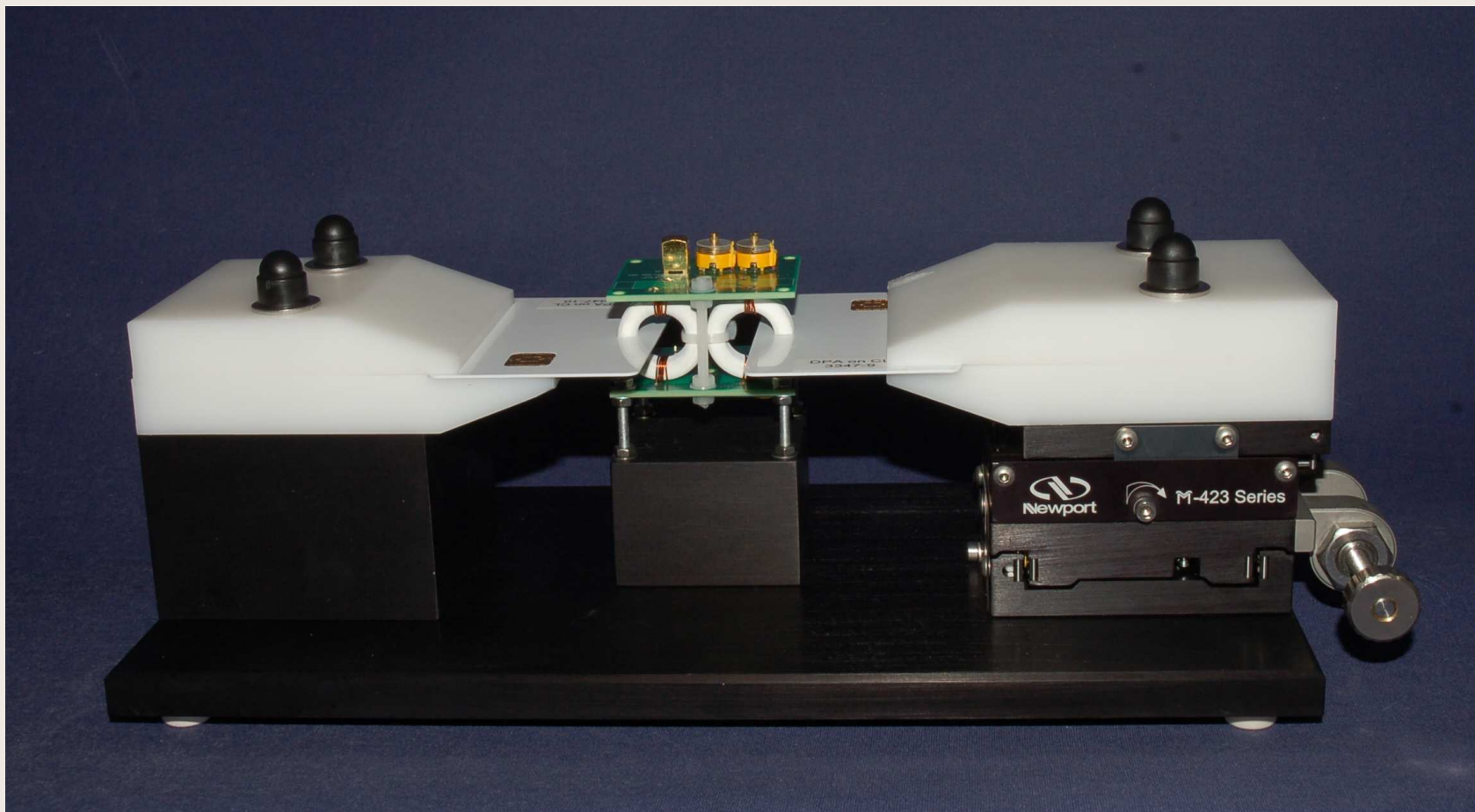
How to measure the power consumption of a contactless card?



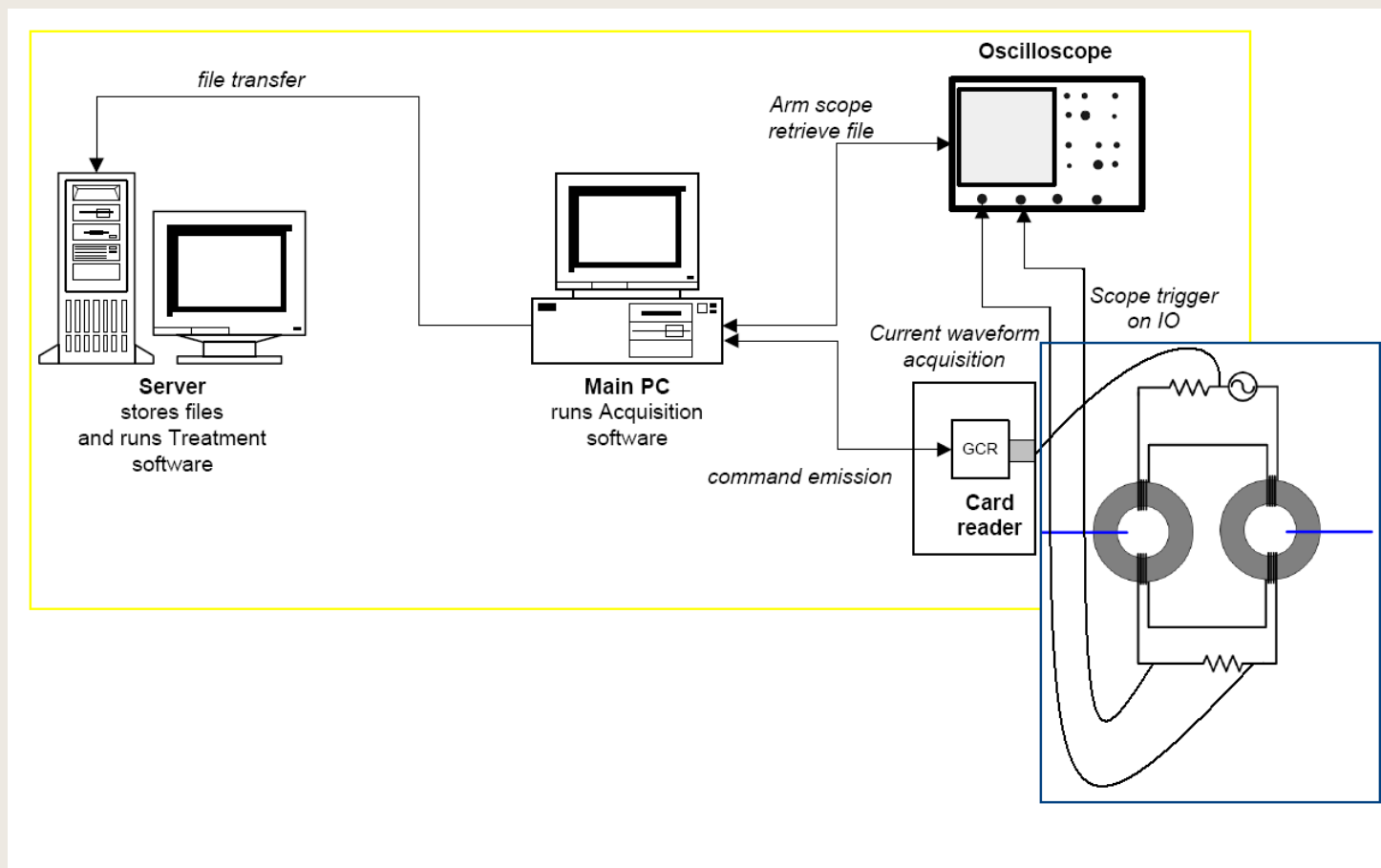
SPA/DPA setup for contactless cards



DPA on Contactless Cards cardholder

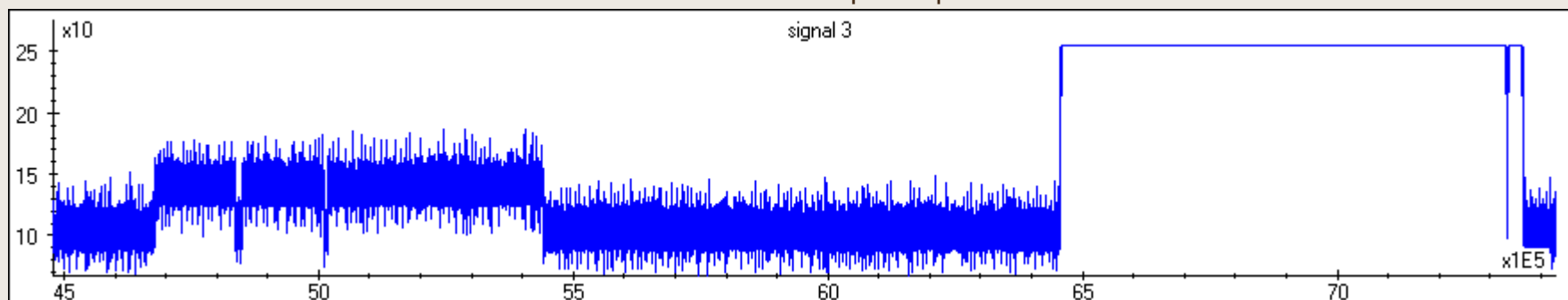


Complete set-up for contact-less DPA

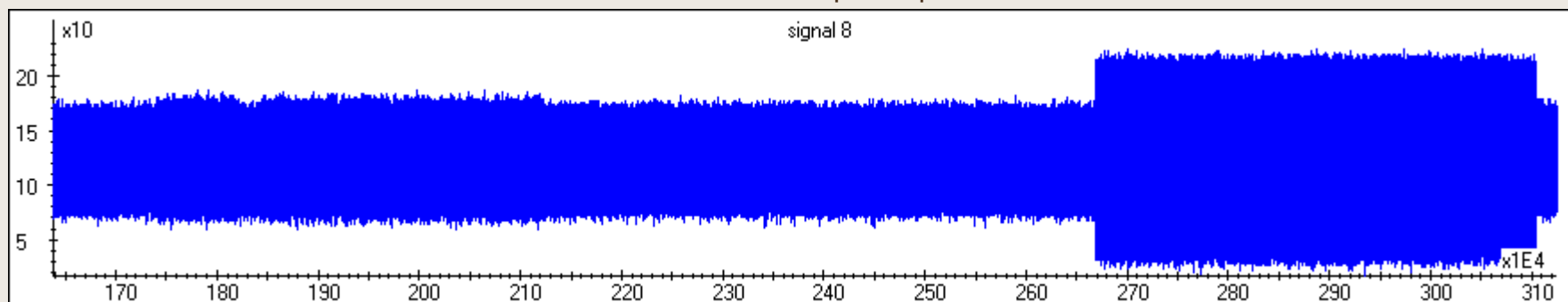


Balanced measurement set-up

Contact interface power profile

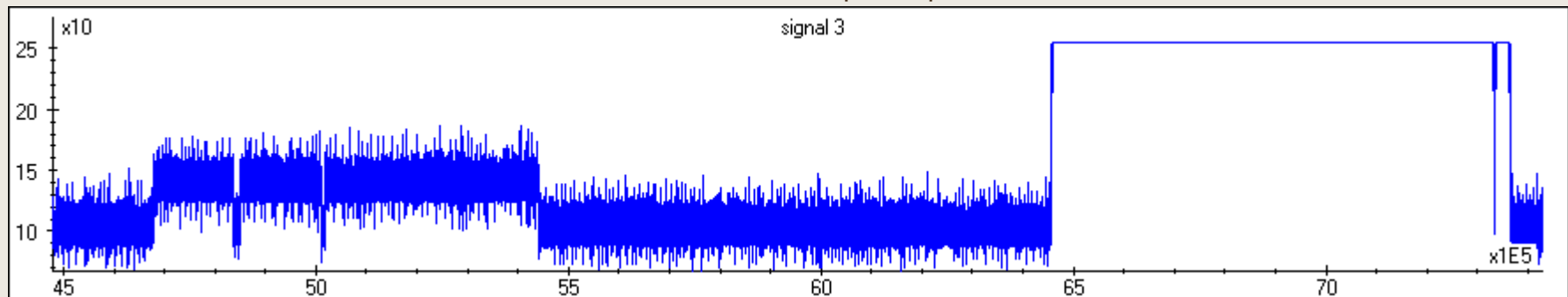


RF interface power profile

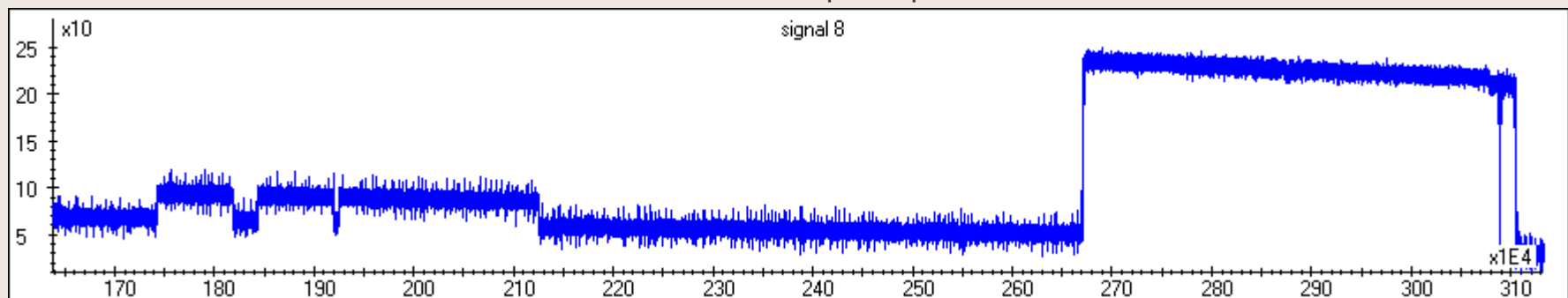


Balanced measurement set-up (after demodulation)

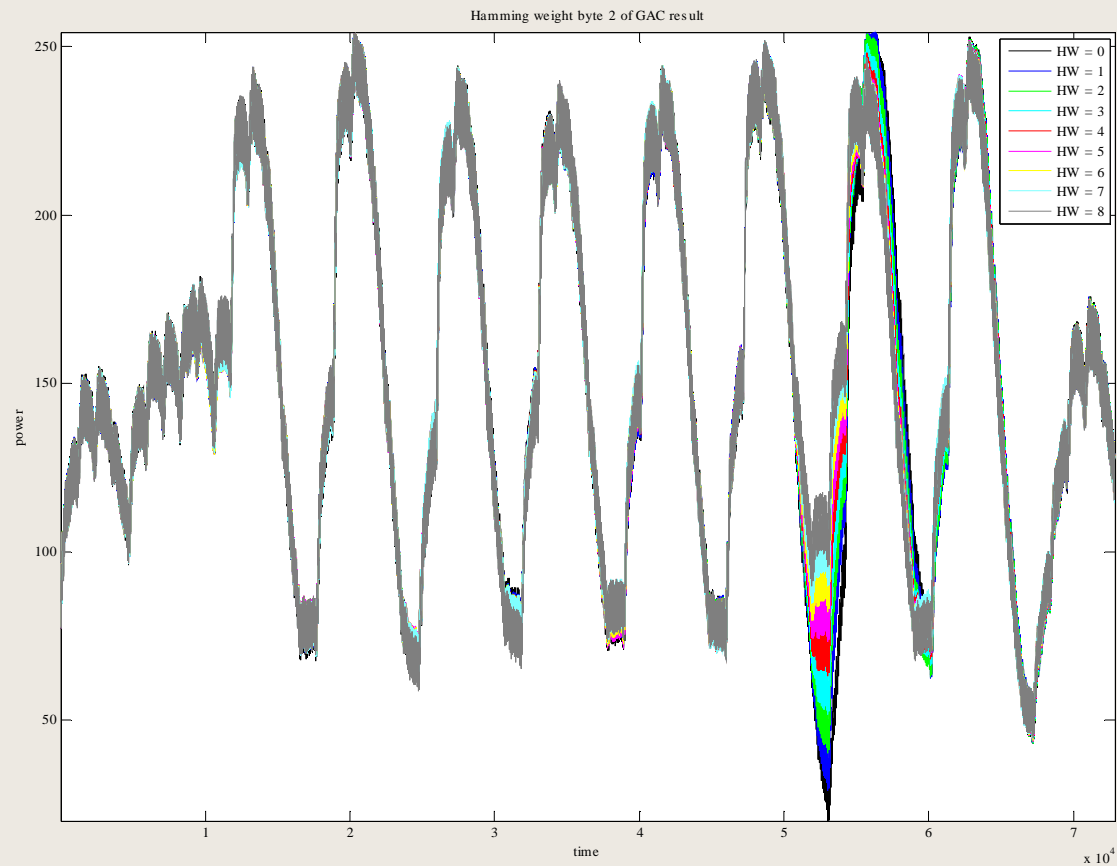
Contact interface power profile



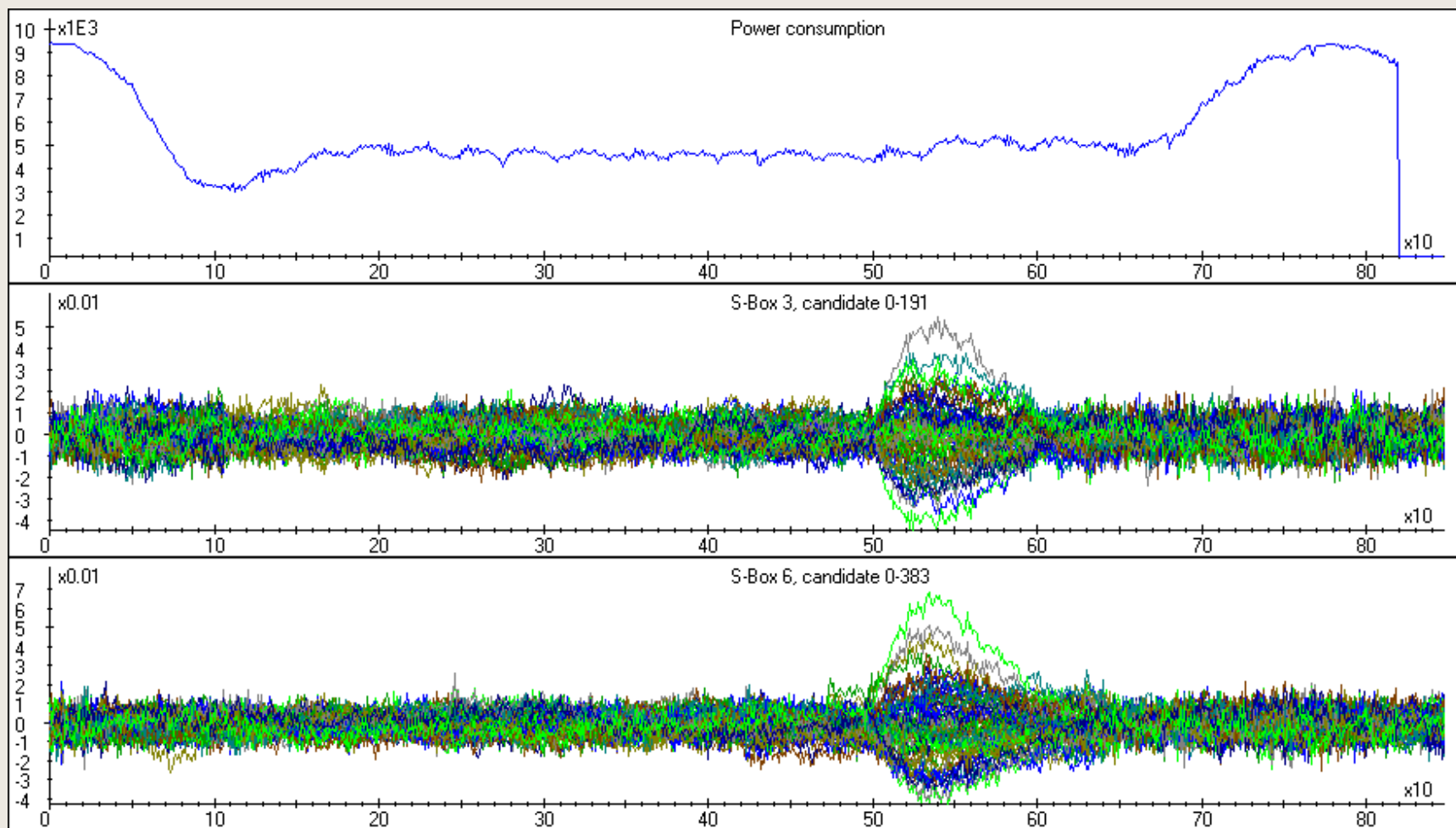
RF interface power profile



SPA/DPA – Hamming weight of processed data



SPA/DPA – DES Co-processor leakage



Attack potential calculation contact DPA on DES

Factor	Comment	Ident'n	Exploit'n
Elapsed Time	Pure data collection of a minimum of 100,000 traces takes at least 3 days. Signal analysis and running the DPA analysis software will take more than a week for the Identification and about a week for the Exploitation phase. (The elapsed time scales roughly linearly with the number of traces taken.)	< 1 month (3)	< 1 month (4)
Expertise	For Identification, the attacker must be an Expert for setting up the measurement and specifying the algorithms for further signal processing. Only a Proficient attacker is required when the attack is repeated in the Exploitation phase.	Expert (5)	Proficient (2)
Knowledge of TOE	In general, we assume that command details are taken from the FSP for the TOE and hence, following [JIL-AP], are Restricted. However, in some cases, where the command specification is freely available (e.g. Global Platform), the knowledge may be Public only.	Restricted (2)	Public (0)
Open Samples / Known Key	It is assumed that open samples are managed appropriately..	Sensitive (4)	Public (0)
Access to TOE	Only a single TOE is required	< 10 Samples (0)	< 10 Samples (0)
Equipment	The equipment includes dedicated equipment built to collect the power traces, a high-end digital oscilloscope, and non-standard, homegrown SPA analysis software.	Specialized (3)	Specialized (4)
Point Subtotal		17	10
Total		27	

Attack potential calculation contact-less DPA on DES

Factor	Comment	Ident'n	Exploit'n
Elapsed Time	Pure data collection of a minimum of 100,000 traces takes at least 3 days. Signal analysis and running the DPA analysis software will take more than a week for the Identification and about a week for the Exploitation phase. (The elapsed time scales roughly linearly with the number of traces taken.)	< 1 month (3)	< 1 month (4)
Expertise	For Identification, the attacker must be an Expert for setting up the measurement and specifying the algorithms for further signal processing. Only a Proficient attacker is required when the attack is repeated in the Exploitation phase.	Expert (5)	Proficient (2)
Knowledge of TOE	In general, we assume that command details are taken from the FSP for the TOE and hence, following [JIL-AP], are Restricted. However, in some cases, where the command specification is freely available (e.g. Global Platform), the knowledge may be Public only.	Restricted (2)	Public (0)
Open Samples / Known Key	It is assumed that open samples are managed appropriately..	Sensitive (4)	Public (0)
Access to TOE	Two TOEs are required	< 10 Samples (0)	< 10 Samples (0)
Equipment	The equipment includes dedicated equipment built to collect the power traces, a high-end digital oscilloscope, and non-standard, homegrown SPA analysis software.	Specialized (3)	Specialized (4)
Point Subtotal		17	10
Total		27	

Practical limitation during contactless operation of smart cards

Contactless operation has two constraints:

- Power:
 - Energy must be transferred 'over the air'
 - Card-to-reader distance is critical
 - Coupling mismatches exist between card and reader
 - Result: less power available compared to contact mode

- Time:
 - Card user responsible for keeping card close to reader
 - In practice: 'card waving' results in short time windows for transaction

Pointers during AVA_VAN: How to deal with, manufacturer 'solutions' to 'solve' limitations

To conserve power and execution time during contactless operation:

- Switch-off power-hungry security countermeasures like current scramblers
- Disable random waitstates to speed-up execution
- Disable countermeasures against DFA like double cryptographic calculation
- Disable countermeasures against perturbation like software flagging

These are real examples!

Result: card can be broken in contactless mode, while secure in contact mode!

conclusion

- DPA on contact-less interface should be considered in AVA_VAN
 - The attack method is mature
 - The measurement method is slightly different requiring two TOEs
 - The DPA analysis is exactly the same as for DPA on a contact interface
 - The contact-less interface is critical on available resources
 - Countermeasures for the contact interface are not always possible for the contact-less interface
 - Introduced countermeasures for the contact-less interface must have similar strength as for the contact interface

Contact information

Monique Bakker

Rob Bekkers

Joachim van den Berg

Bright sight BV

Delftechpark 1

2628 XJ Delft

The netherlands

Tel. : +31-152692500

Fax : +31-152692555

E-mail: info@brightsight.com

url: www.brightsight.com



brightsight®

Questions?

