Side-Channel Analysis (SCA) – A comparative approach on smart cards, embedded systems, and high security solutions

Rohde & Schwarz SIT GmbH

Stuttgart/Germany
Dr. Torsten Schütze

Workshop on Applied Cryptography
Lightweight Cryptography and Side-Channel Analysis
Nanyang Technological University, Singapore
December 3, 2010

ROHDE&SCHWARZ

History of SCA – The smart card world I

(1) P. Kocher: Timing analysis on implementations of DH, RSA, DSS, and other systems, 1995/96.

(2) D. Boneh, R. DeMilo, R. Lipton: On the importance of checking cryptographic protocols for faults, 1996/97.

(3) A. Lenstra: Memo on RSA signature generation in the presence of faults, 1996/97.

(4) E. Biham, A. Shamir: Differential fault analysis of secret key cryptosystems, 1997.

(5) P. Kocher, J. Jaffe, B. Jun: Differential power analysis, 1997/98.

(6) W. Schindler: A timing attack against RSA-CRT, 2000.

(7) J.J.Quisquater, D. Samyde: Electromagnetic anaylsis, 2001.

(8) D. Boneh, D. Brumley: Remote timing attacks are practical, 2003.

(9) S. Chari, C. Jutla, P. Rohatgi: Template attacks, 2003.

(10) E. Brier, C. Clavier, F. Olivier: Correlation power analysis with a leakage model, 2004.

(11) W. Schindler, K. Lemke, C. Paar: A stochastic model for differential side-channel cryptanalysis, 2005.

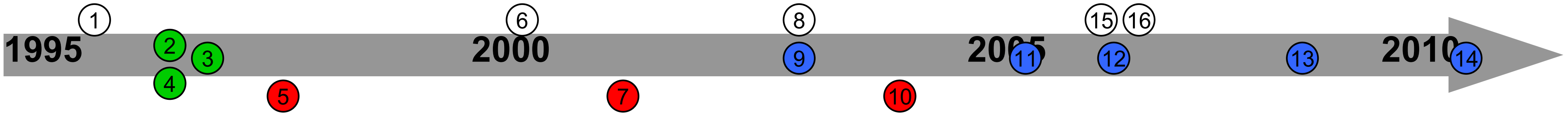
(12) F.-X. Standaert et al.: Template attacks in principal subspaces, 2006.

(13) B. Gierlichs et al.: Mutual Information Analysis, 2008.

(14) J. DiBatista et al.: When failure analysis meets side-channel analysis, 2010

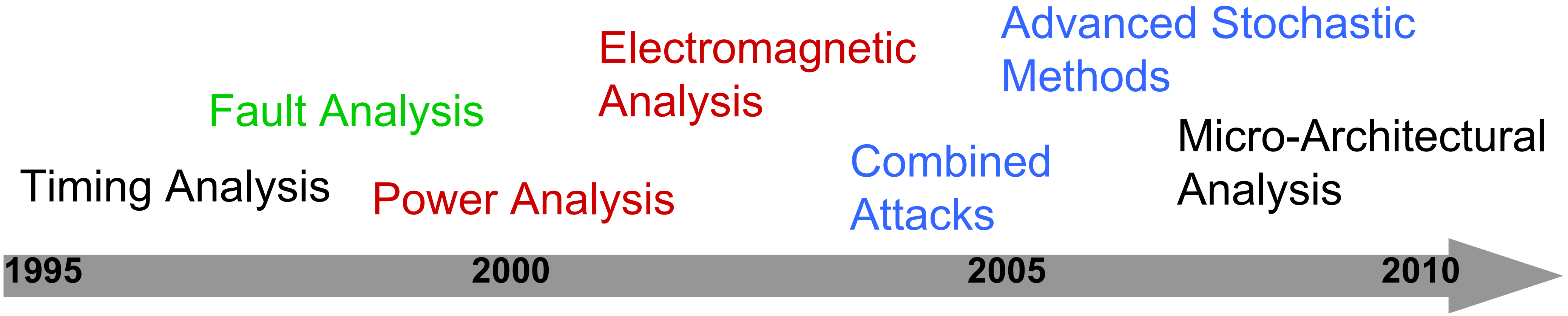
(15) D.J. Bernstein: Cache-timing attacks on AES, 2004/05, D.A. Osvik et al. Cache attacks and countermeasures, 2006.

(16) O. Aciiçmez et al. On the power of simple branch prediction analysis, 2006.



History of SCA – The smart card world II

- ➔ Side-channel attacks hit the smart card industry quite unanticipated
- ➔ Today, we have a myriad of advanced analysis methods available
- ➔ Implementation of efficient hard- and software countermeasures is accepted standard
- ➔ Currently, interesting things at the analysis front happen with advanced stochastic methods and fault attacks


Fault Analysis

Electromagnetic Analysis

Advanced Stochastic Methods

Timing Analysis

Power Analysis

Combined Attacks

Micro-Architectural Analysis

History of SCA – The embedded / automotive world I

(1) Remote Keyless Entry (RKE) since mid of 1990s, Keyless Go since 1999

(2) Immobilizers mandatory in Germany since 1998, in Canada since 2007

(3) Start of tuning protection (=recognition of ECU software modifications) with proprietary methods ~1998

(4) Proprietary authentication methods, end of 1990s

- Break of proprietary methods

(5) Cryptographic tuning protection for some OEMs (RSA PKCS#1 v1.5 signatures with e=3) ~2002

- Man-in-the-Middle attack by exchanging public keys ➔ OTP memory

(6) 2003: Secure odometers, State-of-the-Art authentication by some OEMs

(7) 2005: Researcher break proprietary 40-bit encryption on Texas Instruments transponders

(8) Since 01/2006: Road tolling in Germany, On-Board-Units use certified smart cards, system itself not certified/open yet

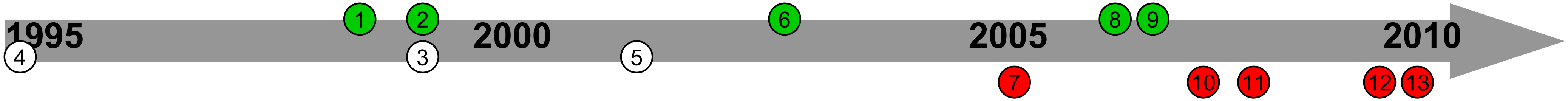
(9) Since 05/2006: Digital Tachograph mandatory in Europe
= first security certified automotive system

(10) 2007 implementation attacks against cryptographic tuning protection in field: Bleichenbacher‘s 2006 attack

(11) 2008: Devastating attack on KeeLoq RKE system using side channel attacks

(12) 2010: Experimental security analysis of a modern automobile ➔ disillusion

(13) Invited talk CHES 2010 – H. Shacham: Cars and voting machines – embedded systems in the field
➔ “They got the simplest cryptographic things wrong!”



History of SCA – The embedded / automotive world II

- Until ~2000, cryptography was not considered very much in the automotive domain
- Currently, automotive is moving from Security by Obscurity to adhering Kerckhoffs‘ law
- University research is starting to consider attacks on automotive security solutions
- Ambitious security challenges ahead with Car2X security ➔ MANET, privacy
- Vulnerability and countermeasures for automotive implementations with respect to SCA currently unknown ➔ Side-Channel Analysis for Automotive Security (SCAAS), see later

“In about ten years, no automotive supplier or manufacturer can afford to build SCA-vulnerable products.”

A. Bogdanov, author of 1st KeeLoq attack paper, 2008.

History of SCA – The high security world

???

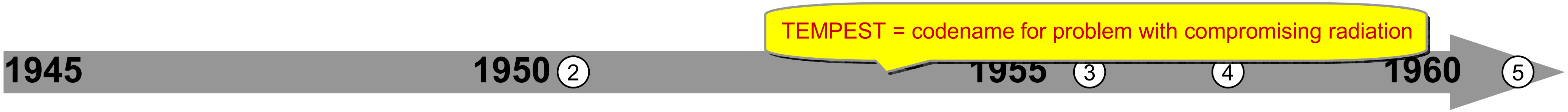
(1) World War I: German army eavesdrop field phone lines observing ground current

(2) 1943/1951: Bell Labs and CIA find electromagnetic side channel in rotor key generator
➔ correlator machines (compute correlation coefficient in hardware)

(3) 1956 suez crisis: MI5 uses acoustic side channel, i.e., clicking of rotors in Haegelin ciphering machine

(4) 1950s: electromagnetic echoes of teleprinter in output of ciphering machine

(5) 1962: Japan captures electromagnetic emanations of American cipher machines



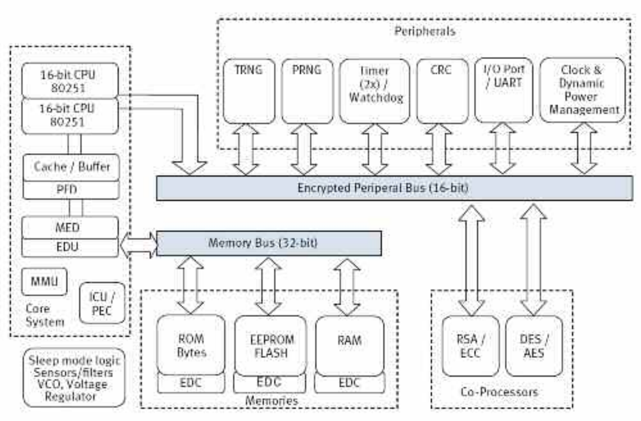
TEMPEST = codename for problem with compromising radiation

- ➔ Red / black separation: separation of systems that handle classified / plaintext information (RED) from those that handle non-classified / encrypted information (BLACK)
- ➔ Radiation policies
  - 1953 US Armed Forces Security Agency (pre-NSA): first TEMPEST policy
  - 1958 first joint policy in US
  - 1959 + UK and Canada ➔ combined policy
- ➔ Today: BSI zoning model (0-3), NATO SDIP-27 Level A-C, actual emission limits are classified
- ➔ Only some of the earliest TEMPEST information has been declassified, most of the actual limits, testing procedures and countermeasures remain secret.
- ➔ First target of TEMPEST: plaintext correlation / absolute radiation limits. Later: key correlations

A comparative analysis – Processors and devices

Smart cards

From 8-bit (SLE66) through 16-bit dual-core (SLE78) to 32-bit high-end (SLE88) processors

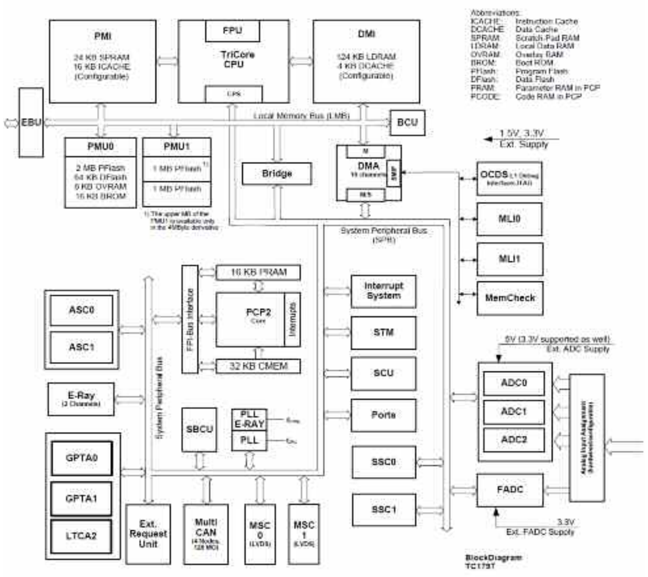


Block diagram Infineon SLE78

-25 ° C to +70 ° C,
some controllers with extended spec (M2M): -40 ° C to +105 ° C

Automotive / Embedded

From 4-bit (key fobs) to 32-bit RISC (Engine Control Units) processors with DSPs; upcoming: 32-bit Multi-Core



Block diagram Infineon TC1797

Operational conditions

-40 ° C to +125/155 ° C (normal/attached to engine) + mechanical shocks + vibration

High security solutions

General Purpose Processors + ASICs + smart cards + FPGAs

???

Ruggedized: MIL-STD-810, protected against electromagnetic pulses

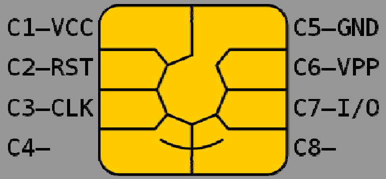
Problem with standard security ICs

A comparative analysis – Interfaces

Smart cards

Contact-based	Contactless
ISO 7816-3, T=0, T=1; serial halfduplex protocols	ISO 14443, 13.56 MHz radio frequency

New cards: USB, Single Wire Protocol

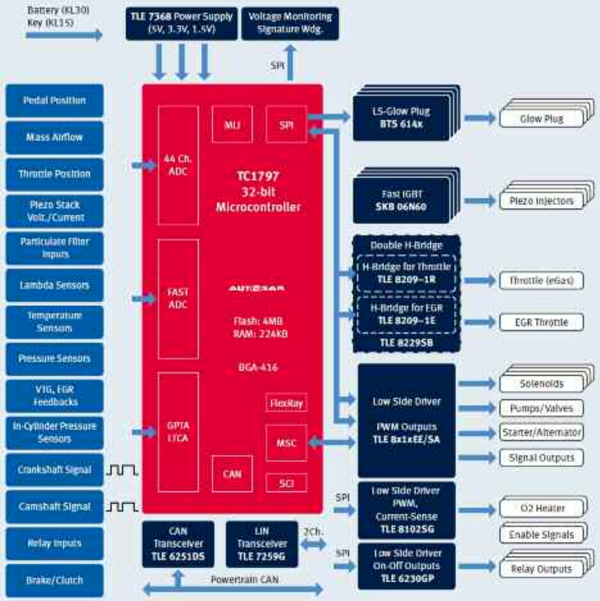


Interfaces for contact-based smart card

Relatively uniform, widely interoperable over APDUs

Automotive / Embedded

LIN, CAN, Flexray, MOST,…
Asynchronous Serial Channels
Synchronous Serial Channels
JTAG, etc.



Interfaces from Infineon TC1797 in Diesel Engine Management

Wide range of high performance interfaces

High security solutions

External: crypto interface
= fill device using serial DS-101 / DS-102 protocol
= military protocol to load cryptographic keys into crypto devices, uses U-229 audio connector plug
Internal: many interfaces to smart cards, FPGAs, ASICs

R&S MMC3000 multimode encryption device (voice, data)

R&S GP3000 Fillgun (data load device)

A comparative analysis – Security features

Smart cards

- Dual CPUs for fault detection
- Full CPU, memory, bus and cache encryption/masking
- Error detection codes
- Dual-rail pre-charge logic, some vendors asynchronous logic, masked logic
- TDES/AES hardware coprocessors
- Crypto@2304T asymmetric coprocessor (RSA, ECC)
- Pseudo RNG and True RNG, AIS-31 and FIPS140 compliant
- Watchdogs for program flow
- Sensors: voltage, frequency, temperature, light
- Active shield

Automotive / Embedded

- Currently, almost no built-in security
- One Time Programmable memory + watchdogs
- No secure non-volatile memory
- Cryptographic security in software

Upcoming:

- Processors with cryptographic coprocessors (mostly symmetric – AES, TRNG)
- = ideas for Secure Hardware Extensions

- Secure NVM and general non-functional security not in focus (cost reasons), functionality counts (and is easy) → crypto accelerators

High security solutions

- Everything from smart cards

+

- Anti-tamper shielding
- Red/black separation
- Optical links to avoid electromagnetic cross-talk
- Filtering to reduce signal to noise ratio
- Power compensation techniques

1960s (!!) TEMPEST documents:

(a) **Shielding**
(b) **Filtering**
(c) **Masking**

MIL-HDBK-232A: Red/black isolation depends fundamentally on proper **Grounding, Bonding, and Shielding**

TEMPEST – Notion and countermeasures

- Codename for problem with compromising radiation, approx. since 1953
- Sometimes, Tiny ElectroMagnetic Particles Emitting Secret Things ☺
- Later, name for several NSA projects
- Today, big industry (over 1 billion per year), everything with compromising radiation

Countermeasures already proposed by Bell Labs

(a) Shielding

- = encapsulation of radiating equipment, establishment of zones
- problem: expensive, problems with heat dissipation

(b) Filtering

- = filter out compromising frequencies/signals
- problem: compromising emanations occur in large portion of frequency spectrum; varying between machines and different environments
- filers have to be near perfect ➔ expensive + heavy

(c) Masking

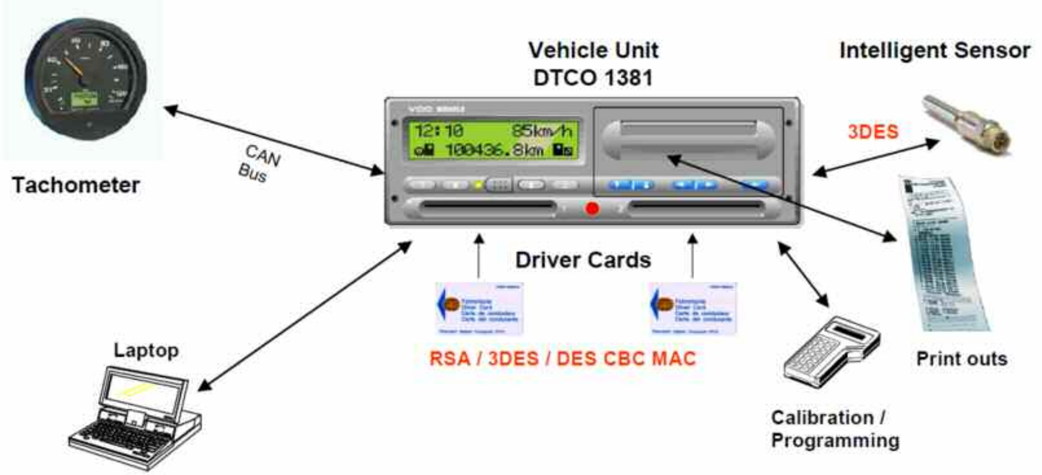
- = deliberately creating a lot of ambient electrical noise to overcome, jam or smear out the offending signals
- problem: just adding white noise is not enough

A comparative analysis – Attack potential and costs

Smart cards	Automotive / Embedded	High security solutions
Access to the target ❙ Directly exposed to the attacker	❙ Often protected by mechanical means, no security shielding	❙ Tamper proof with shielding, armed soldiers and other organizational measures ❙ Crypto Ignition Key – used to declassify equipment
Expertise of the attacker ❙ From layman to expert (Pay TV)	❙ From layman (owner of the car) to expert (tuning mafia)	❙ Multiple experts (intelligence)
Necessary equipment ❙ From standard to bespoke	❙ From standard to specialized	❙ Bespoke/multiple bespoke
Know-how and documentation ❙ Confidential user manuals, published algorithms	❙ Often still Security by Obscurity	❙ Even radiation limits and algorithms / domain parameters are classified, classified doc
Number of pieces and costs ❙ 4.5 billion processor cards 2009 ❙ High-volume, price sensitive	❙ 51 million cars worldwide 2009 ❙ Very price sensitive	❙ ??, ~100.000? per year ❙ Security counts, not very price sensitive
Lifetime ❙ ≤ 5-10 years	❙ ≤ 20-25 years	❙ ??, very old legacy systems

Example 1: Digital Tachograph[$]

- Old system: analogue tachograph charts mandatory in Europe for commercial vehicles since 1985
- New system: digital tachograph mandatory in Europe since 05/2006 (new trucks and buses) detect tampering with driving and rest times
- **First ITSEC E3 high / Common Criteria EAL4+ certified automotive system**
- Uses smart card technology, focus of Siemens CT work: Cryptography of Vehicle Unit and Motion Sensor
- Main security problem: Side-channel resistance!!
- Our results: SPA/DPA/DFA-protected implementation of DES/RSA on C167 compatible processor, 16 bit, 25MHz



[$] work at Siemens Corporate Technology for SiemensVDO, now Continental AG/Schaeffler

Example 2: SCA-protected AES-implementation on TC1796 §

Processor

- IFX TriCore 1796/1797 32-bit RISC@150/180 MHz
- = processor in Engine Control Units
- 2 MByte program flash, 128 kByte data flash, 136 kByte data memory, 16 kByte instruction cache, scratchpad RAM

➔ Not bad?! But:

- Crypto budget is much smaller, especially RAM
- No secure non-volatile memory

  ➔ Low cost countermeasures
- Algorithm runs in time-slots with lot of noise

Countermeasures

- First order masking

  ➔ Which scheme? Dozens of proposals, see *Secure and Efficient Masking of AES – a Mission Impossible?* Oswald:Mangard:Pramstaller 2004
- Shuffling: randomize the number of S-box first evaluated
- Operations on dummy cycles: insert dummy S-box evaluations

Remarks on countermeasures:

- 8-bit scheme proposed: Herbst:Oswald:Mangard:2006
- 32-bit extension: Tillich:Herbst:Mangard:2007
- ➔ scheme is not resistant to higher order attacks, see Tillich:Herbst:2008

Implementation results

- Investigation of various masking schemes using abstract processor model
- Optimized implementation of 8-bit countermeasures (masked SubBytes as S-box) on 32-bit platform, results from THM07 not applicable (HW instruction set extension)

- ➔ medium security high-speed AES-128 implementation
- ➔ not yet evaluated/measured
- ➔ scratch pad RAM may lead to Micro-Architectural timing attacks
- ➔ measurements in SCAAS project

§ joint work with A. Hoheisel, Bochum University, 2009.

SCA public funded projects in Germany

- German Federal Ministry of Education and Research: Call for IT security research in 2009
- “New methods for side-channel analysis” becomes focus area
- Two projects with participation of author and Rohde & Schwarz SIT, respectively.

Side Channel Analysis for Automotive Security (SCAAS)

SCAAS - Side Channel Analysis for Automotive Security

- Partners:

RUHR UNIVERSITÄT BOCHUM RUB

escrypt Embedded Security

Hochschule Bonn-Rhein-Sieg

BOSCH

- Start: 1.1.2011
- Public funding: 1.08 mio EUR
- Focus:
  1. What is the attack potential of SCA in Automotive Security and Safety?
  2. Specific attack potential on unprotected implementations on typical processors
  3. Adoption of countermeasures
  4. Effectivity and efficiency of implemented countermeasures

RESIST – Methods and tools for securing embedded and mobile systems against next generations attacks

RESIST

- Partners:

Fraunhofer SIT

Bundesamt für Sicherheit in der Informationstechnik

Giesecke & Devrient

TECHNISCHE UNIVERSITÄT DARMSTADT

RUHR UNIVERSITÄT BOCHUM RUB

infineon

escrypt Embedded Security

ROHDE&SCHWARZ

- Start: 1.7.2010
- Public funding: 2.78 mio EUR
- SIT focus: build evaluation platform for Side-Channel Analysis for Software, FPGAs and Smart Cards with red/black separation, optical links, measurements against V_{io}, V_{aux} (in addition to V_{ground})
- = kind of SASEBO[1] for government / high security applications

[1] Side-channel Attack Standard Evaluation Board

Conclusions

- **“TEMPEST [or side-channel analysis] difficulties seem to whipsaw us more than any of the other technical security problems we have.”**

  David G. Boak Lectures, 101 pages, 1966, revised 1973, p. 39,
  NSA COMINT SECRET, declassified 2008-12-10.

- **Side-channel attacks and countermeasures are now relatively well understood in high security solutions and smart card world, but as always in security/cryptography it is an ongoing race.**

- **The automotive / embedded world is just starting to catch up; currently SCA is just a R&D issue, not product relevant yet.**