Do It Yourself: Power Analysis

OpenSource Security Ralf Spenneberg

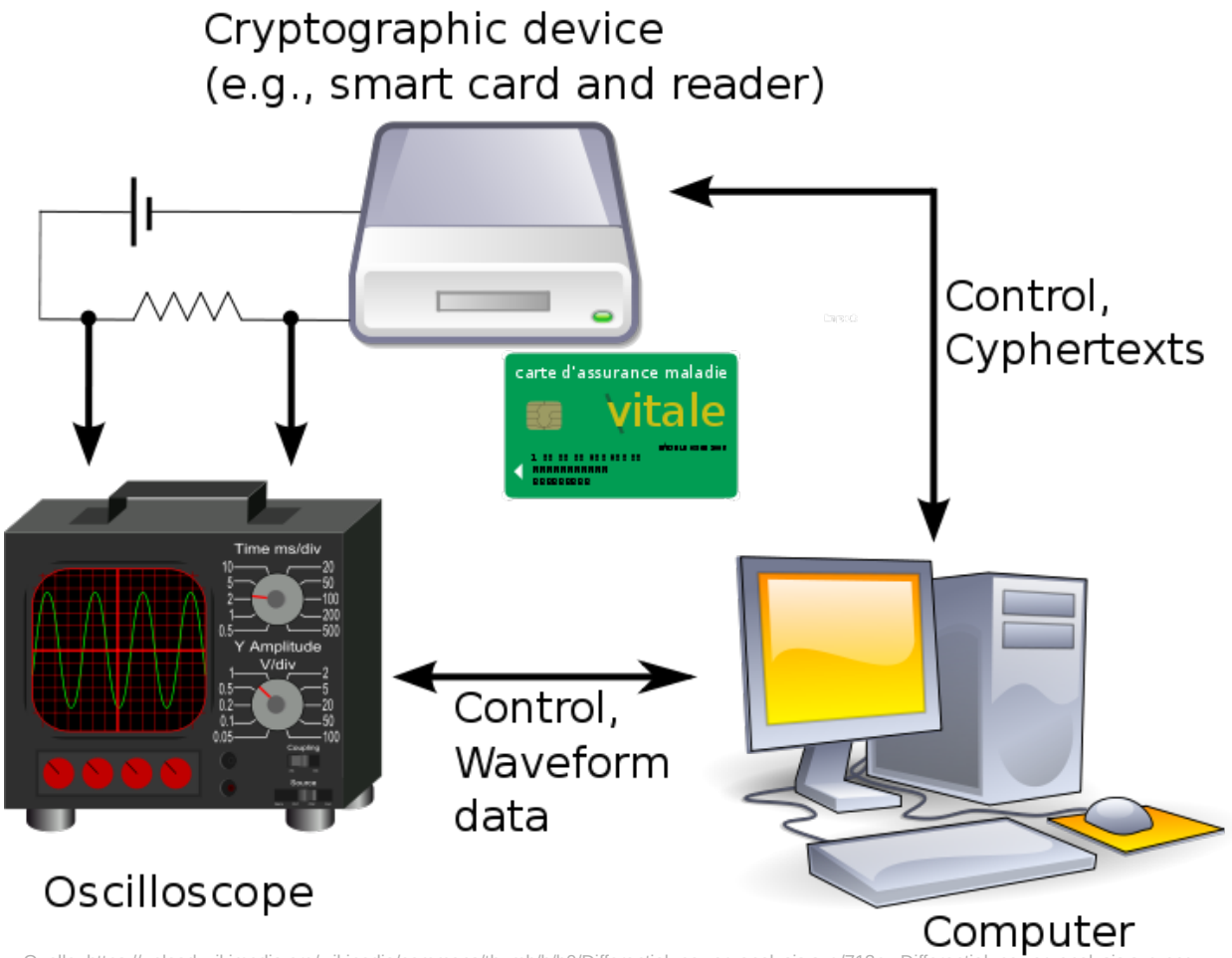
Seitenkanalangriff

- Angriff auf ein kryptographisches System
- Bereits seit 1996 bekannt (Paul C. Kocher)
- Nutzt physikalische Messgrößen
- Beruht auf Korrelationen zwischen beobachteten Daten und hypothetischen Annahmen über den Schlüssel

Seitenkanalangriff – Beispiele

- Timing Attack
  - Messung der Rechenzeit
- Electromagnetic Attack
  - Messung von elektromagnetischen Feldern
- Power-Analysis
  - Messung der Stromaufnahme

Power-Analysis Attacks (1/2)



Quelle: https://upload.wikimedia.org/wikipedia/commons/thumb/b/b0/Differential_power_analysis.svg/713px-Differential_power_analysis.svg.png

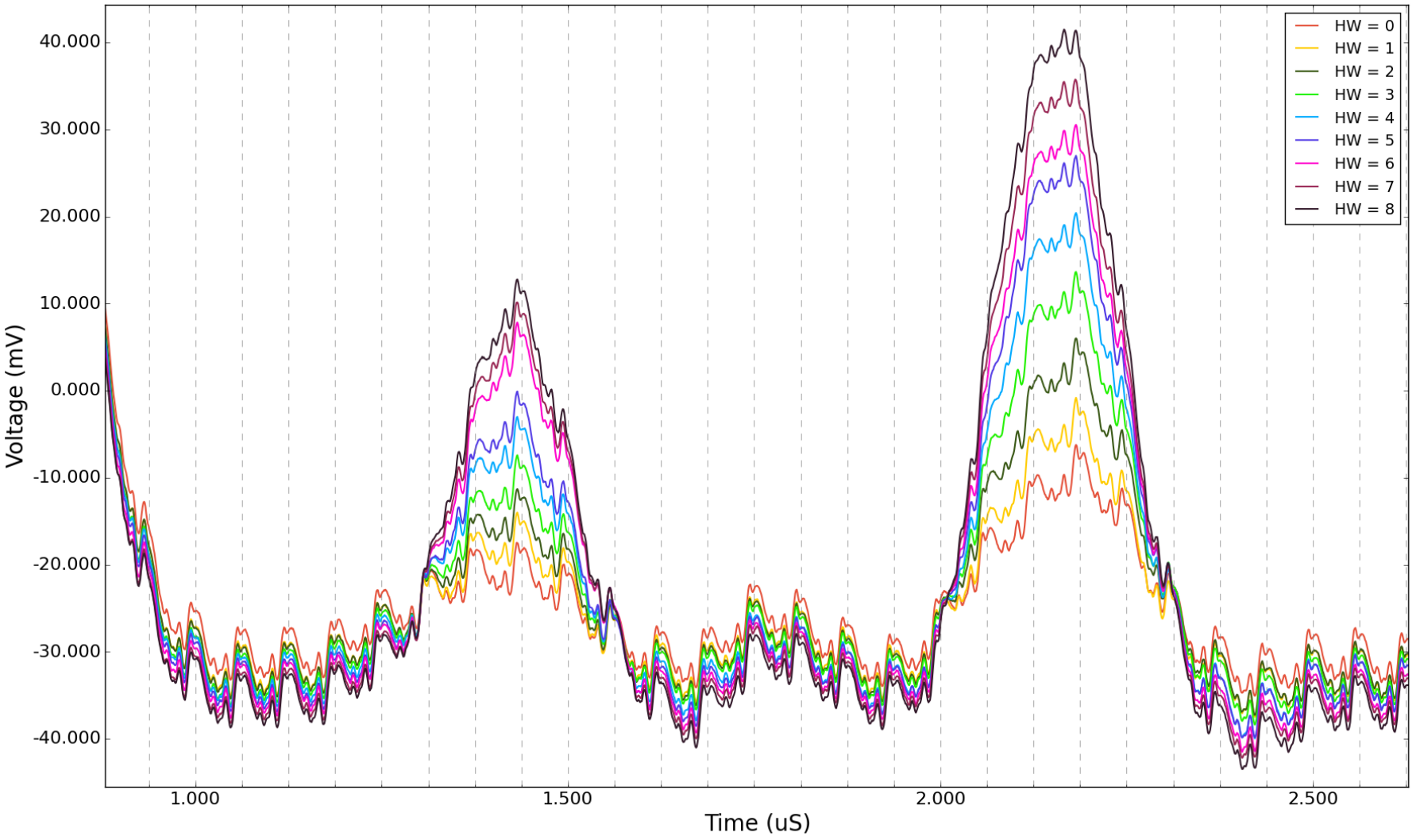
Power-Analysis Attacks (2/2)

- Aufzeichnen der Leistungsaufnahme eines Gerätes während einer kryptographischen Operation
- Passiv
- Nutzt die folgenden Umstände:
  - Stromverbrauch ist abhängig von der ausgeführten Operation
  - Stromverbrauch ist abhängig von den Daten

Power-Analysis Attacks – Prinzip

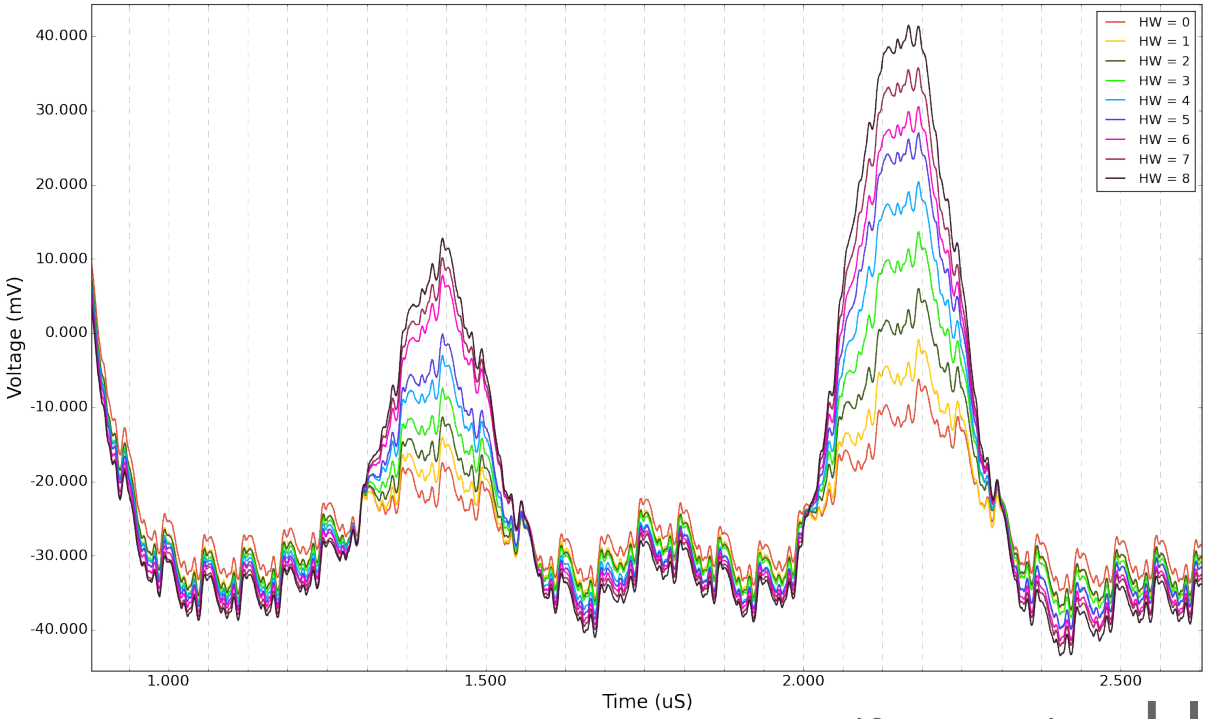
- Datenbus benötigt Strom (Statisch, Dynamisch)

Power-Analysis Attacks – Prinzip

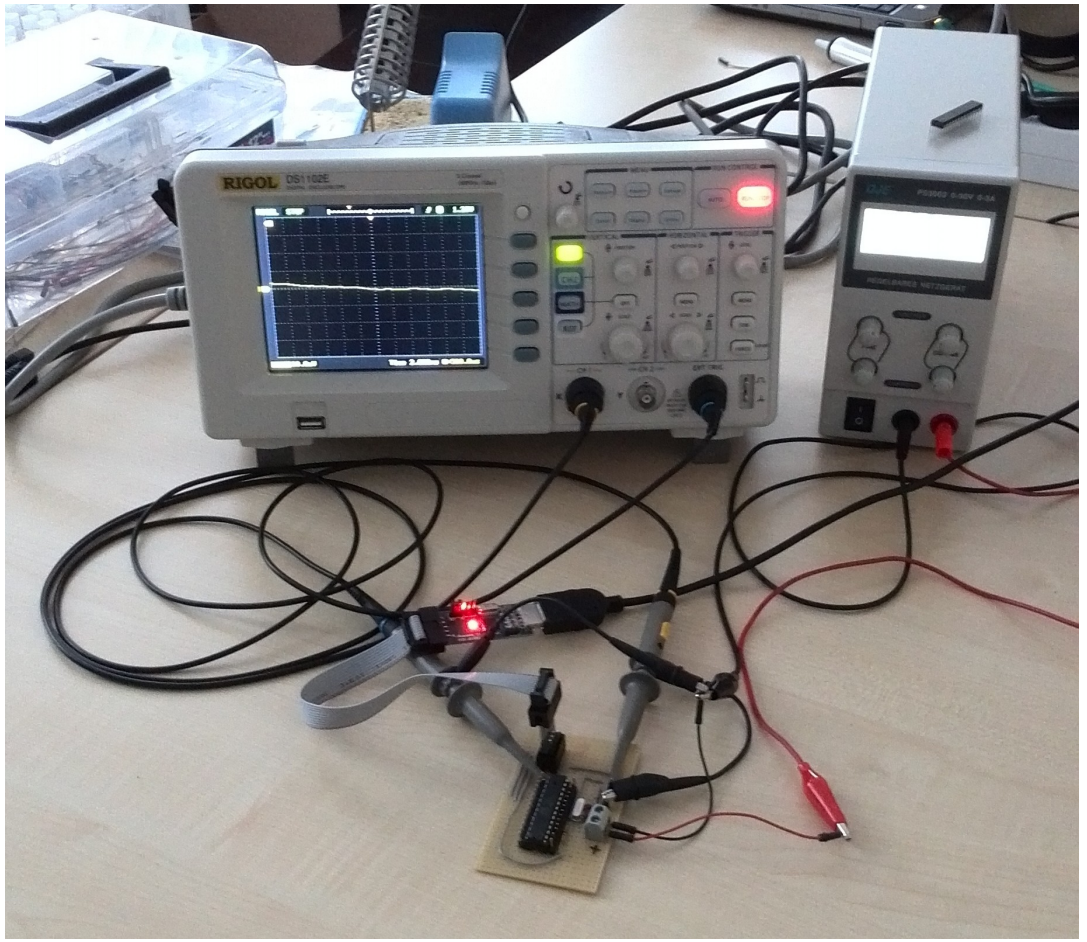


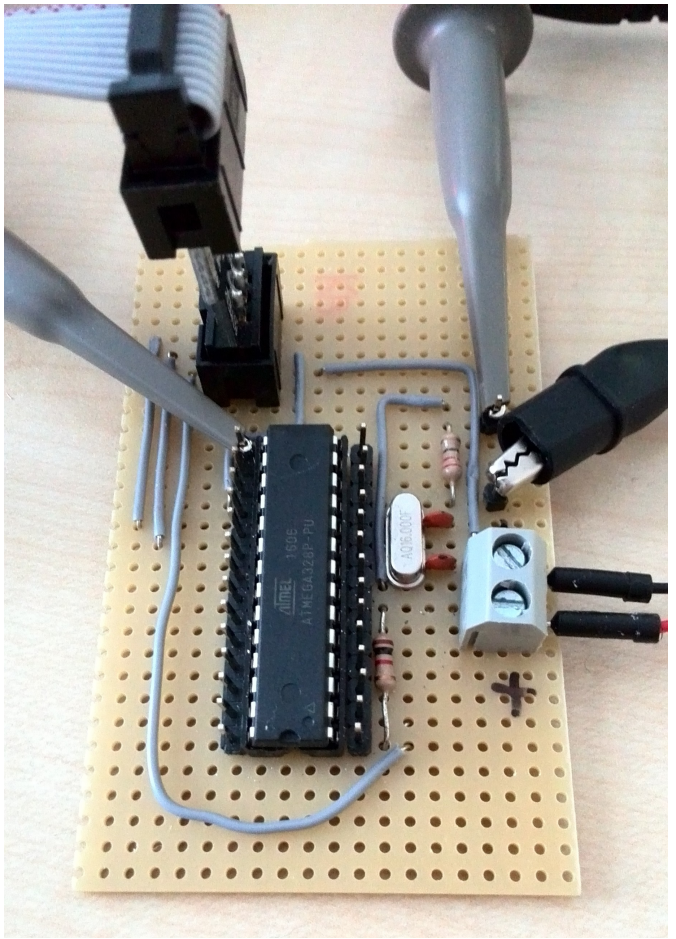
Power-Analysis Attacks – Prinzip

- Datenbus benötigt Strom (Statisch, Dynamisch)
- Stromverbrauch ist proportional zur Anzahl der gesetzten Bits auf dem Datenbus



Laboraufbau





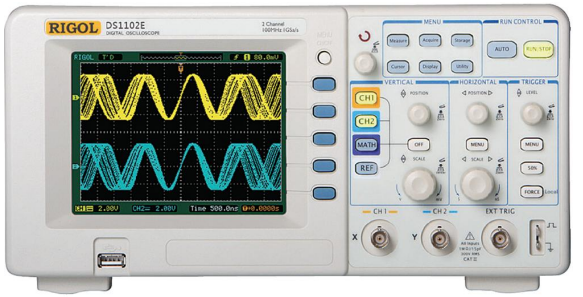
Verwendete Hardware

- Microcontroller (ATmega88A, ATmega328P)
- USB In-Circuit-Programmer (USBasp)
- Regelbares Netzgerät (QJE PS3003)
- Digitaloszilloskop (Rigol DS1102E) ~400€
- [Grafikkarte (GeForce GTX 970) ~300€]

Hardware – Kenngrößen

- Microcontroller
  - Flash-Speicher
  - RAM
- Oszilloskop
  - Bandbreite
  - Abtastrate
  - Datenübertragungsrate

Quelle:
http://store.synthrotek.com/assets/images/atmega88a-ic.jpg



Quelle:
https://img.conrad.de/medias/global/ce/1000_1999/1200/1220/1224/122423_BB_00_FB.EPS.jpg

Verwendete Software

- Oszillokop
  - Gut dokumentierte Schnittstelle
  - ASCII-Code basiert
- Grafikkarte
  - PyCUDA
- Eigenentwicklung (python)

Power-Analysis Attacks – Verfahren

- Simple Power Analysis (SPA)
  - Visuelle Analyse
- Differential Power Analysis (DPA)
  - Statistische Analyse

SPA

- Visuelle Analyse der Messungen
- Einige wenige Messungen der Stromaufnahme
- Voraussetzungen:
  - Genaue Messung (kein / wenig Rauschen)
  - Kenntnis über Implementierung

SPA – Beispiel (1/2)

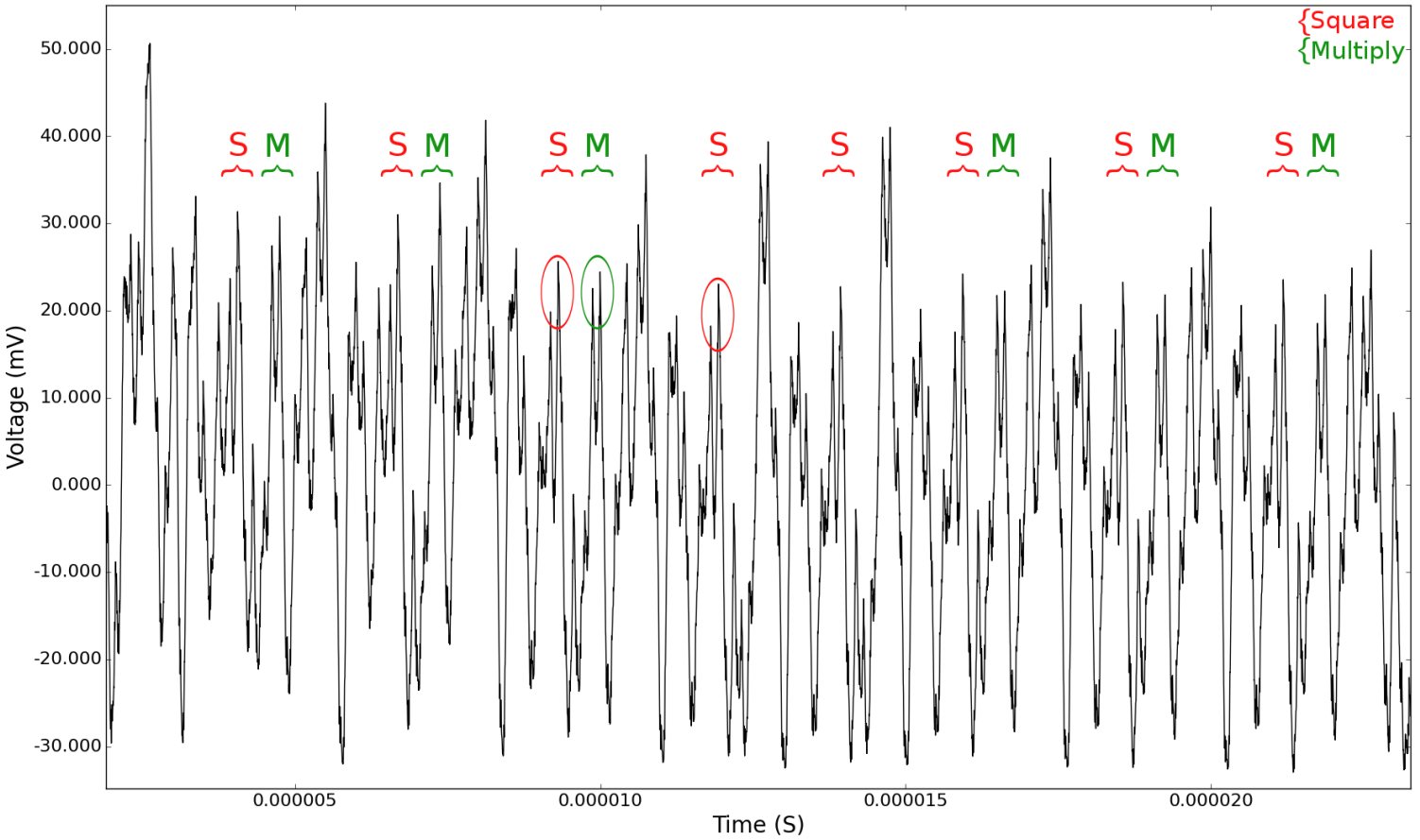
- RSA-Kryptosystem
  - Verschlüsselungsverfahren
  - Signaturverfahren
- Beispiel:

$$231_{10} = 11100111_2$$

$$7^{231} = ((((((((1^2 * 7)^2 * 7)^2 * 7)^2)^2)^2 * 7)^2 * 7)^2 * 7$$

- Square-and-Multiply

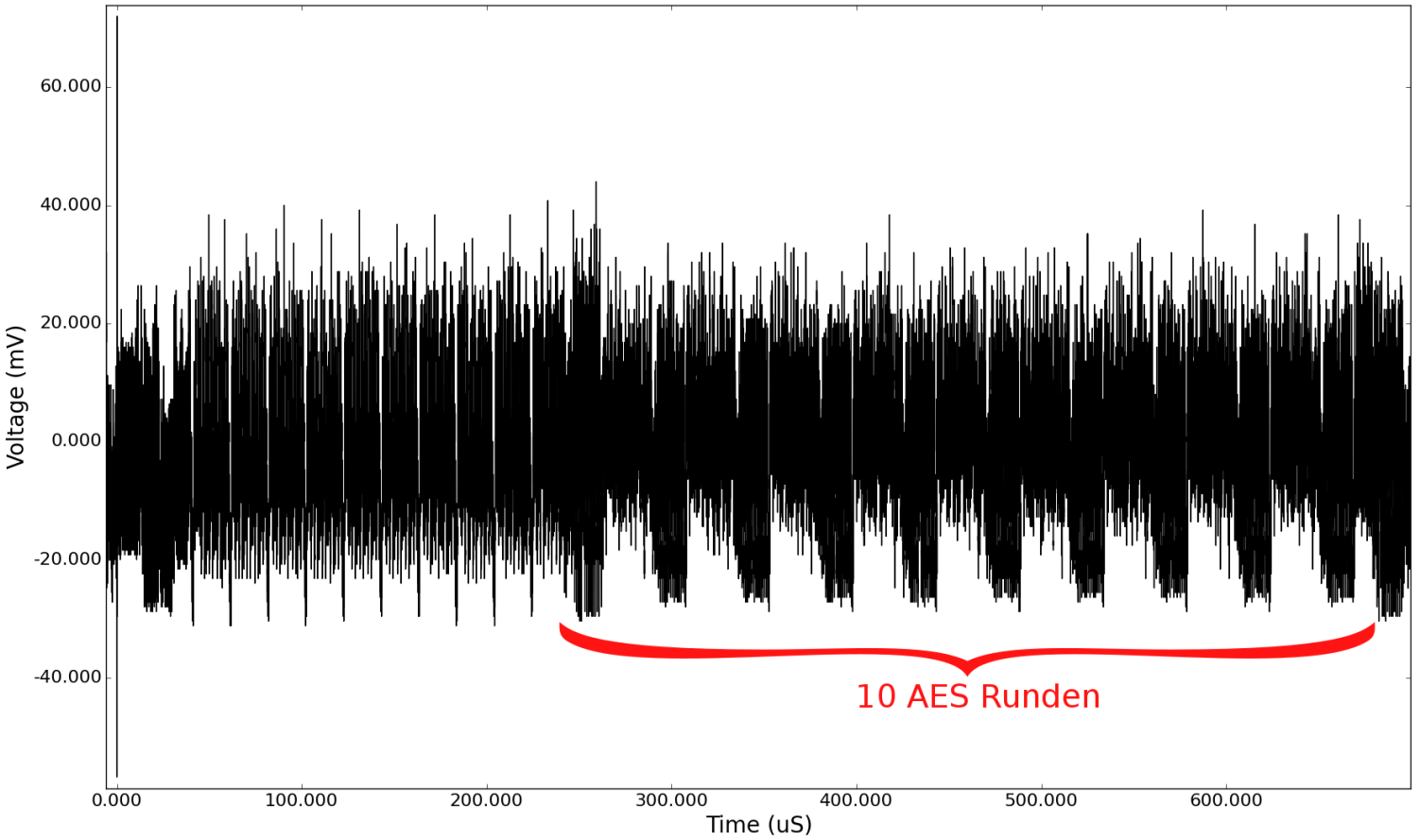
SPA – Beispiel (2/2)



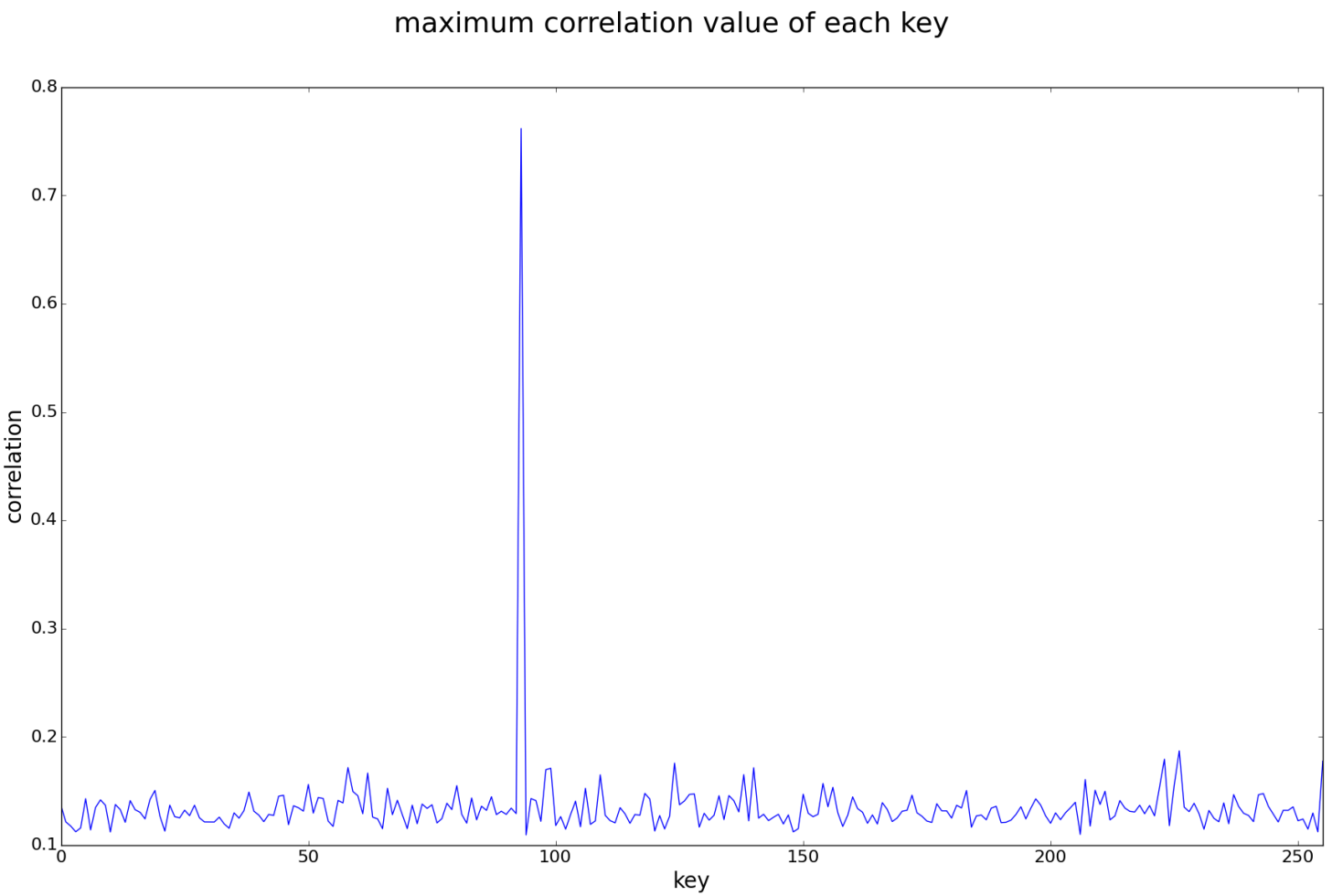
DPA

- Setzt statistische Methoden ein
- Benötigt große Anzahl an Messungen der Stromaufnahme
- Voraussetzungen:
  - Kryptographische Operation muss bekannt sein
  - Klartext oder Chiffrat muss bekannt sein
- „Correlation Power Analysis“ (CPA)

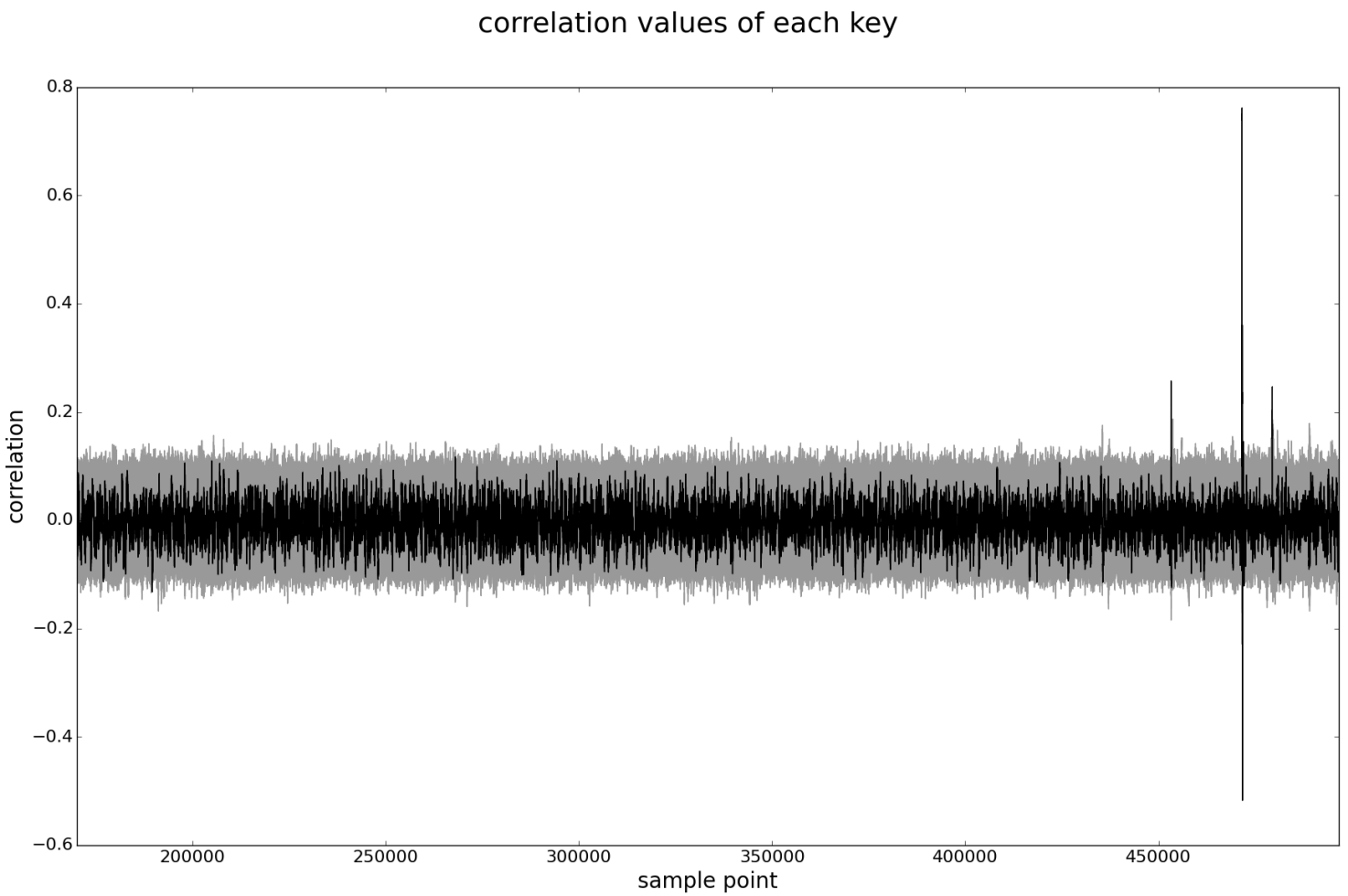
DPA – Beispiel (1/3)



DPA – Beispiel (2/3)



DPA – Beispiel (3/3)

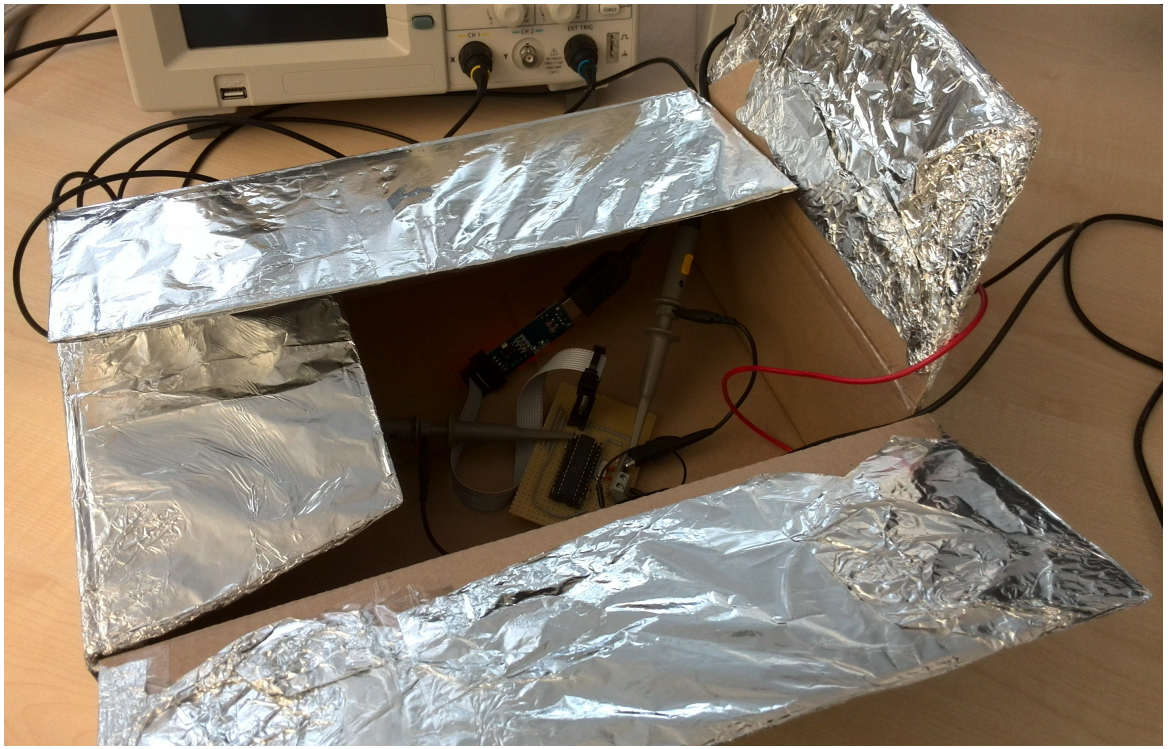


Zeitfaktoren

- Oszilloskop
  - Ca. 90min für 1000 Traces (1024^2 Messpunkte)
- CPU vs. GPU
  - CPU: 32 Kerne, ~ 8h
  - GPU: 1664 CUDA Recheneinheiten, ~ 5min

Herausforderungen / Lösungsansätze (1/2)

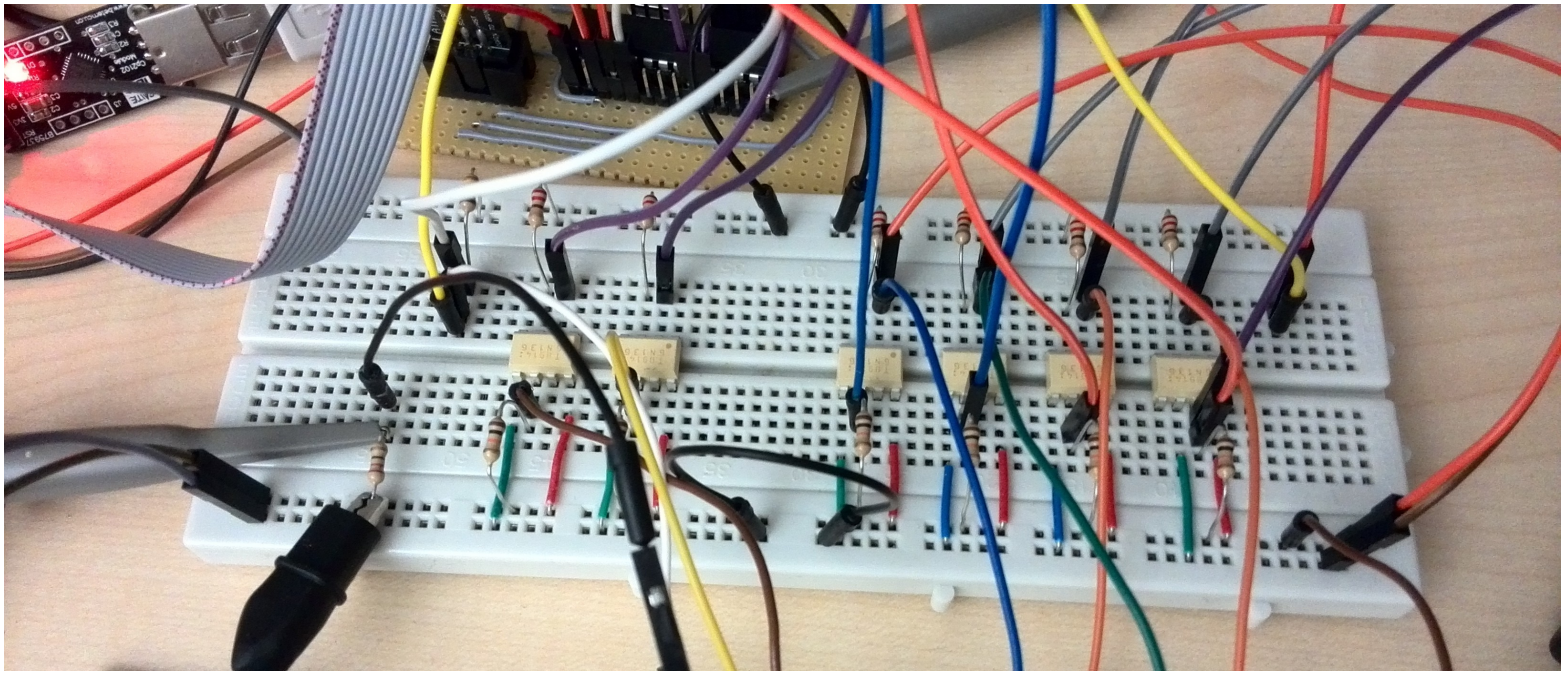
- Netzgerät → Batterie
- Verschobene Traces
- Alubox



Praktisches Anwendungsbeispiel

Herausforderungen / Lösungsansätze (2/2)

- Transistor
- Optokoppler

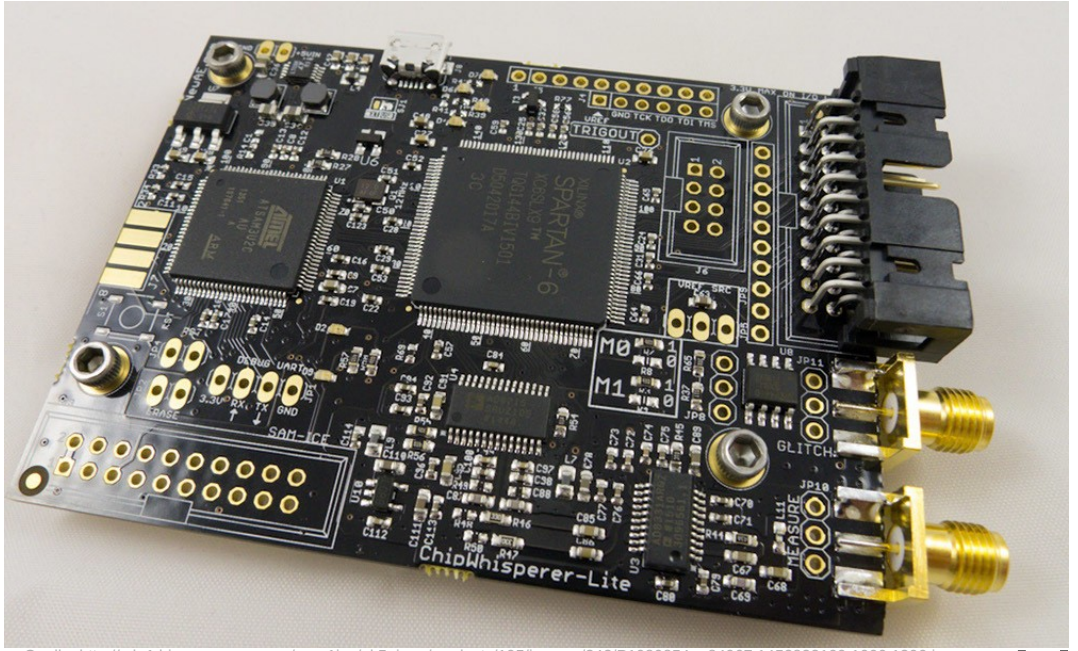


ChipWhisperer-Lite (1/3)

- Kickstarter Projekt (Colin O'Flynn)
- Toolchain bestehend aus Hardware und Software
- Bietet z.B. die Möglichkeit zum Durchführen von Power Analysis Attacks

ChipWhisperer-Lite (2/3)

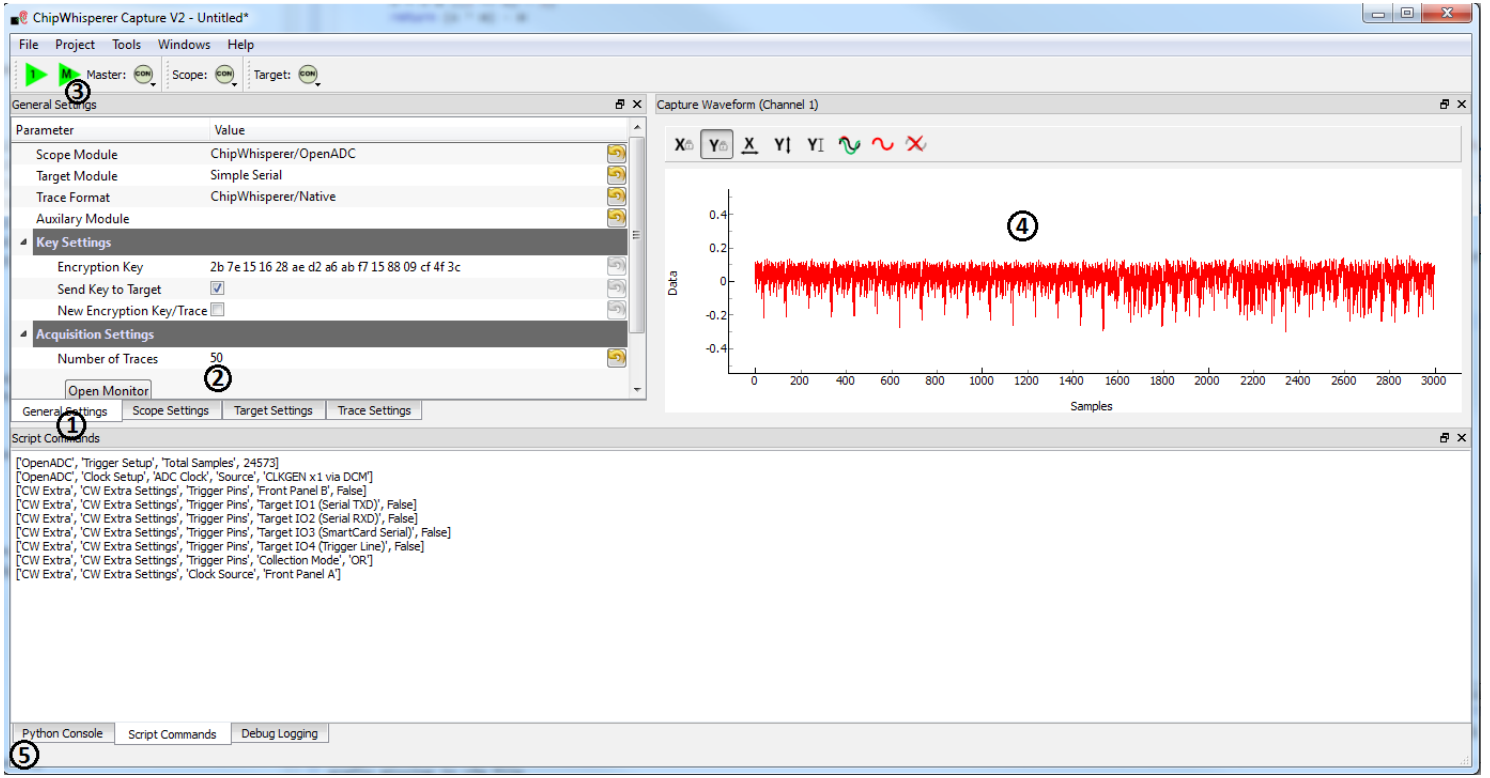
- ChipWhisperer-Lite (CW1173)
- XMEGA Target Board
- Advanced Breakout Board (CW506)
- Differential Probe



Quelle: http://cdn1.bigcommerce.com/n-ou1isn/pk5aiywx/products/105/images/342/P1080854__84967.1452822199.1000.1200.jpg

ChipWhisperer-Lite (3/3)

- ChipWhisperer Capture
- ChipWhisperer Analyzer



Quelle: http://chipwhisperer.readthedocs.io/en/latest/_images/capture.png

Gegenmaßnahmen

- Verschleierung des Klartexts / Chiffrats
- Dummy Operationen → Desynchronisation
- Vermeidung bedingter Sprünge
- Einfügen von Rauschen
- Dual-Rail-Precharge-Logic

Do It Yourself: Power Analysis

Erich Klundt
erich@os-s.de

OpenSource Security Ralf Spenneberg