Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Seitenkanalangriffe - Praxis und Theorie

Dr. Dominik Klein, Dr. Friederike Laus, Prof. Dr. Werner Schindler

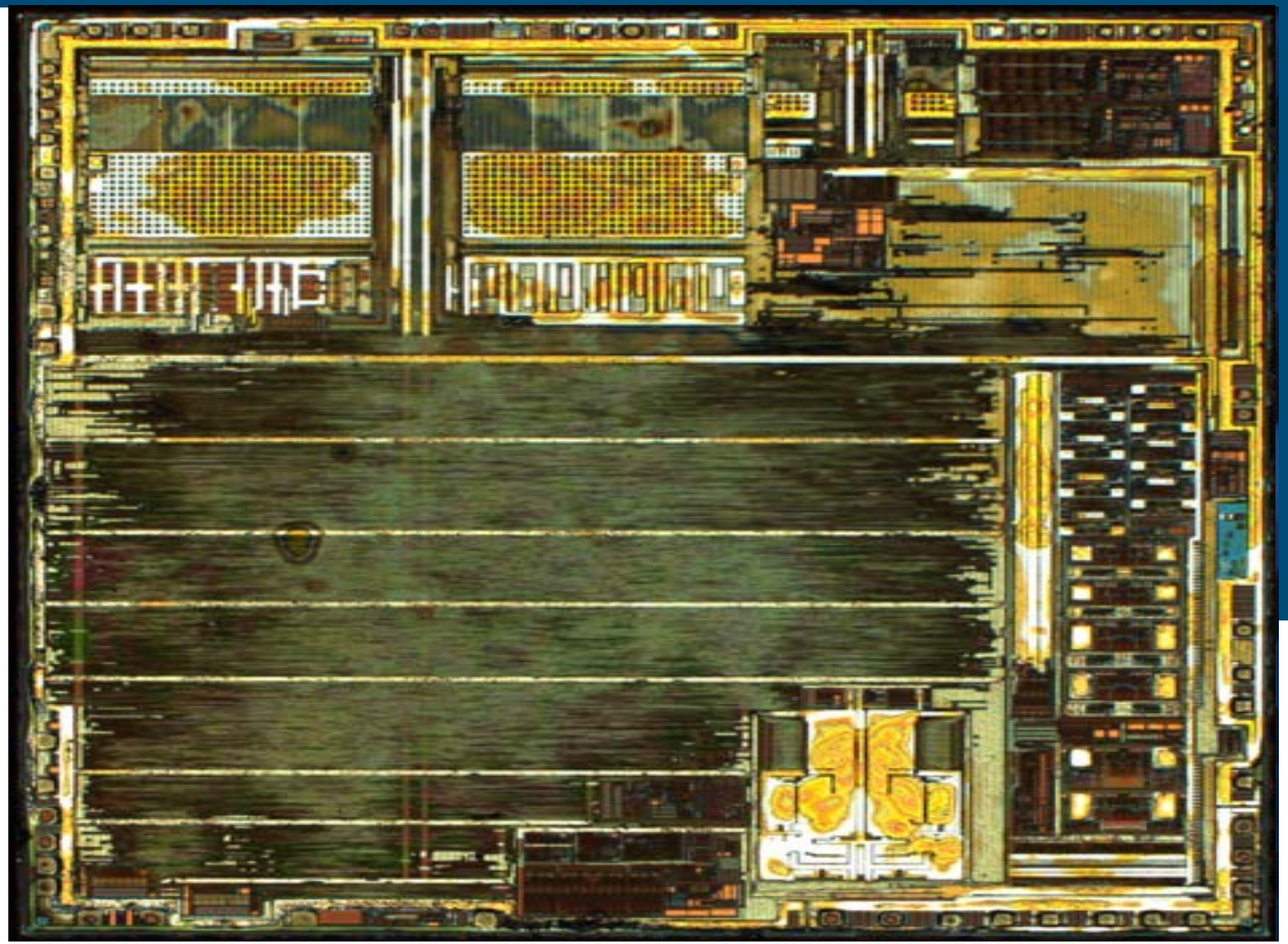
Bundesamt für Sicherheit in der Informationstechnik

Omnisecure 2022

Berlin, den 21.06.2022

Gliederung

- Einführung
- Teil I: Praxis
- Teil II: Theorie
- Zusammenfassung und Ausblick



25 Jahre Seitenkanalangriffe

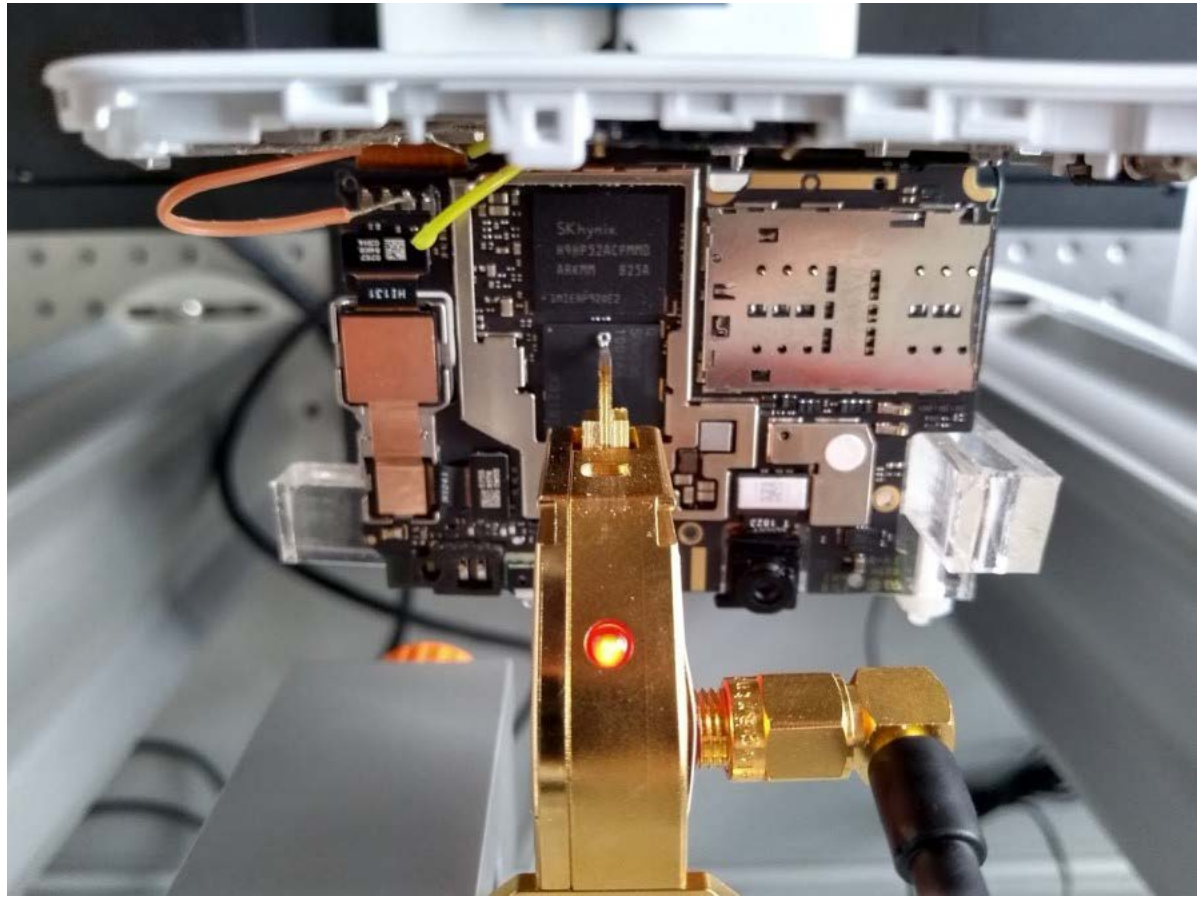
- erste öffentliche Aufsätze zur Seitenkanalanalyse
  - Laufzeitangriffe (Kocher 1996)
  - Powerangriffe (Kocher et al. 1999)
- seitdem:
  - bei jeder hardwarenahen Kryptographietagung gibt es Vorträge zu Seitenkanalangriffen
  - Thema ist für akademische Forschung und Industrie von hohem Interesse
- Seitenkanalgriffe nutzen normalerweise schnittstellenübergreifende Schwachstellen
- kryptographische Schwachstellen resultieren oft aus mangelnder Seitenkanalresistenz
- „Mathematik trifft Ingenieurskunst“

Aktivitäten des BSI

- Zertifizierung und Zulassung
- AIS 46
- eigenes Hardwarelabor
- akademische Erfolge:
  - CHES ist die weltweit größte hardwarenahe Kryptographietagung
  - am Rande der CHES finden jährlich sogenannte Challenges (Wettbewerbe) statt
  - 2018 + 2020: Seitenkanal-Challenges
    - 2018: BSI-Team gewinnt zwei (von sechs) Teil-Challenges
    - 2020: BSI-Team gewinnt alle Preise, die vergeben werden
  - zahlreiche Aufsätze in einschlägigen Fachjournalen und Tagungsbänden

Teil I: Praxis

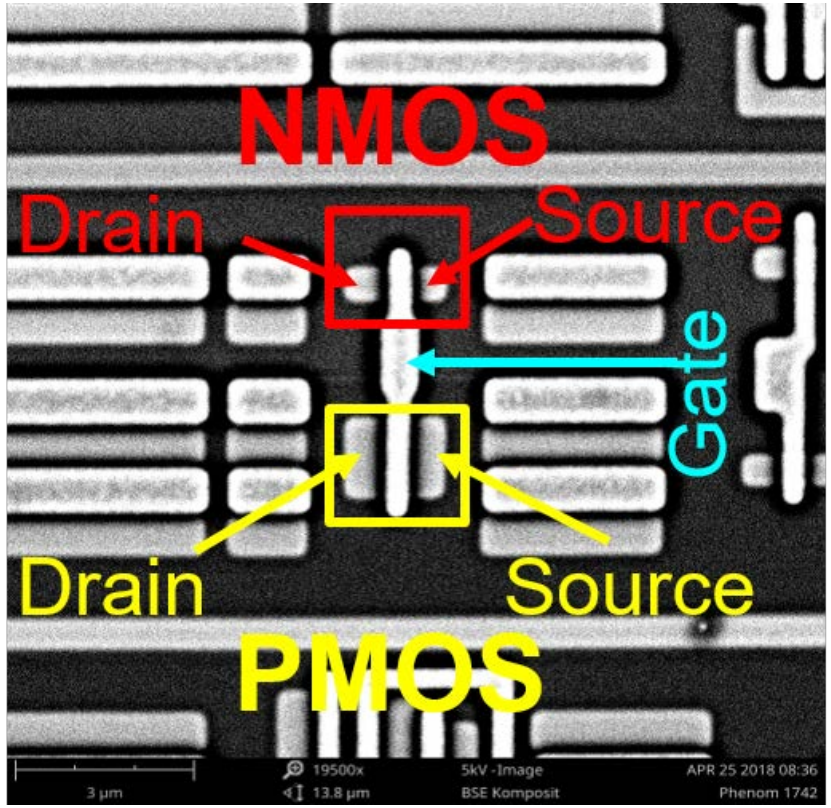
- Wodurch entsteht Leakage?
- Präparation des Chips
- Identifikation der Leakage
  - örtlich
  - zeitlich
- Gegenmaßnahmen



Wodurch entsteht Leakage?

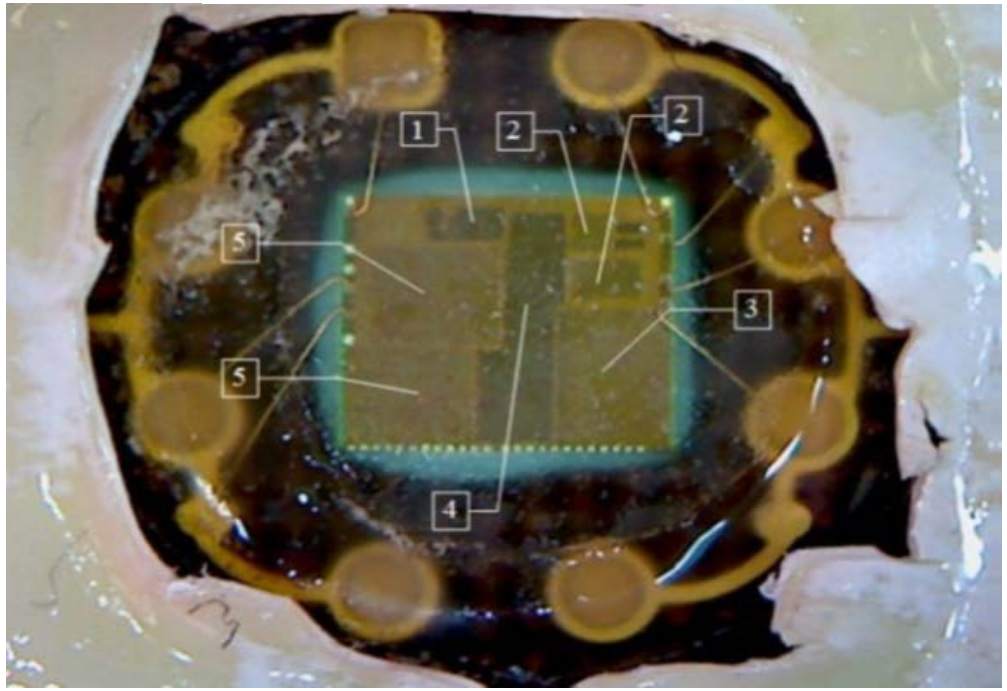
Schaltvorgang	Stromverbrauch
1 → 0	Hoch
0 → 1	
1 → 1	Niedrig
0 → 0	

Verhalten von CMOS/FinFET/FD-SOI Schaltungen (vereinfacht)



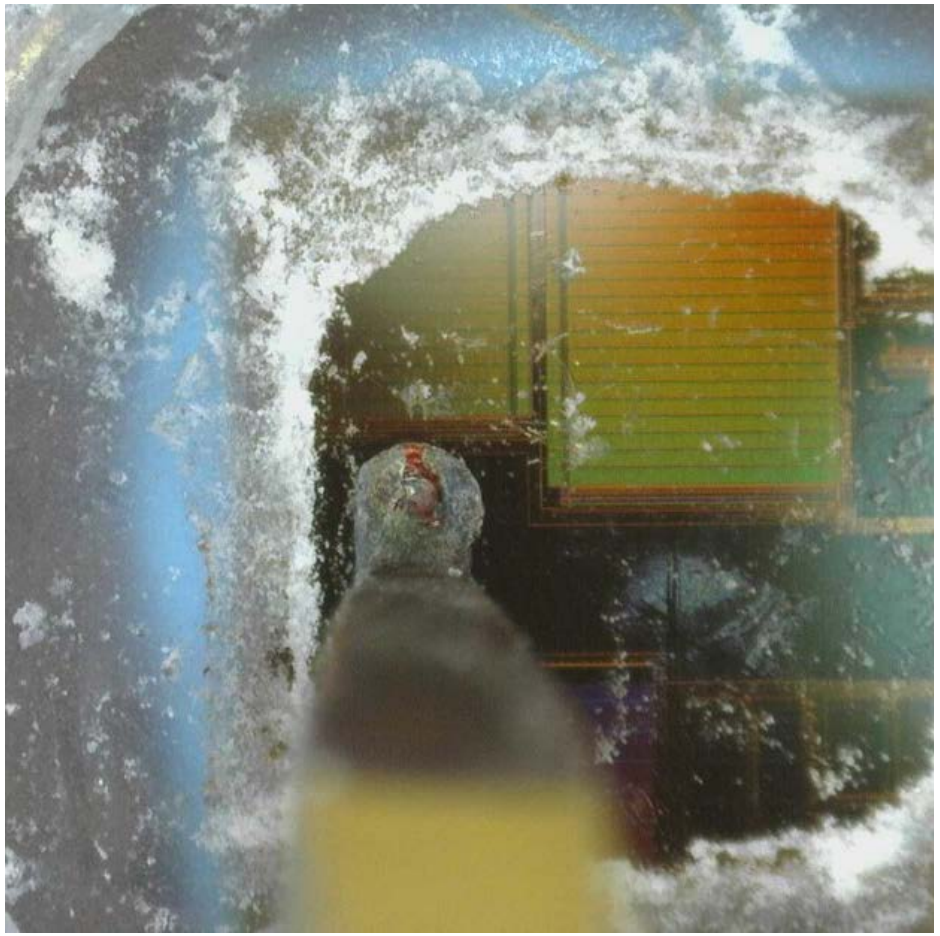
Präparationsschritte

- **Vergussmasse & Plastik**
- **Lösungsmittel**
- **Rauchende Salpetersäure**
- Metallseite: (Re)-Bonding
- Siliziumseite: Dünnen des Chips



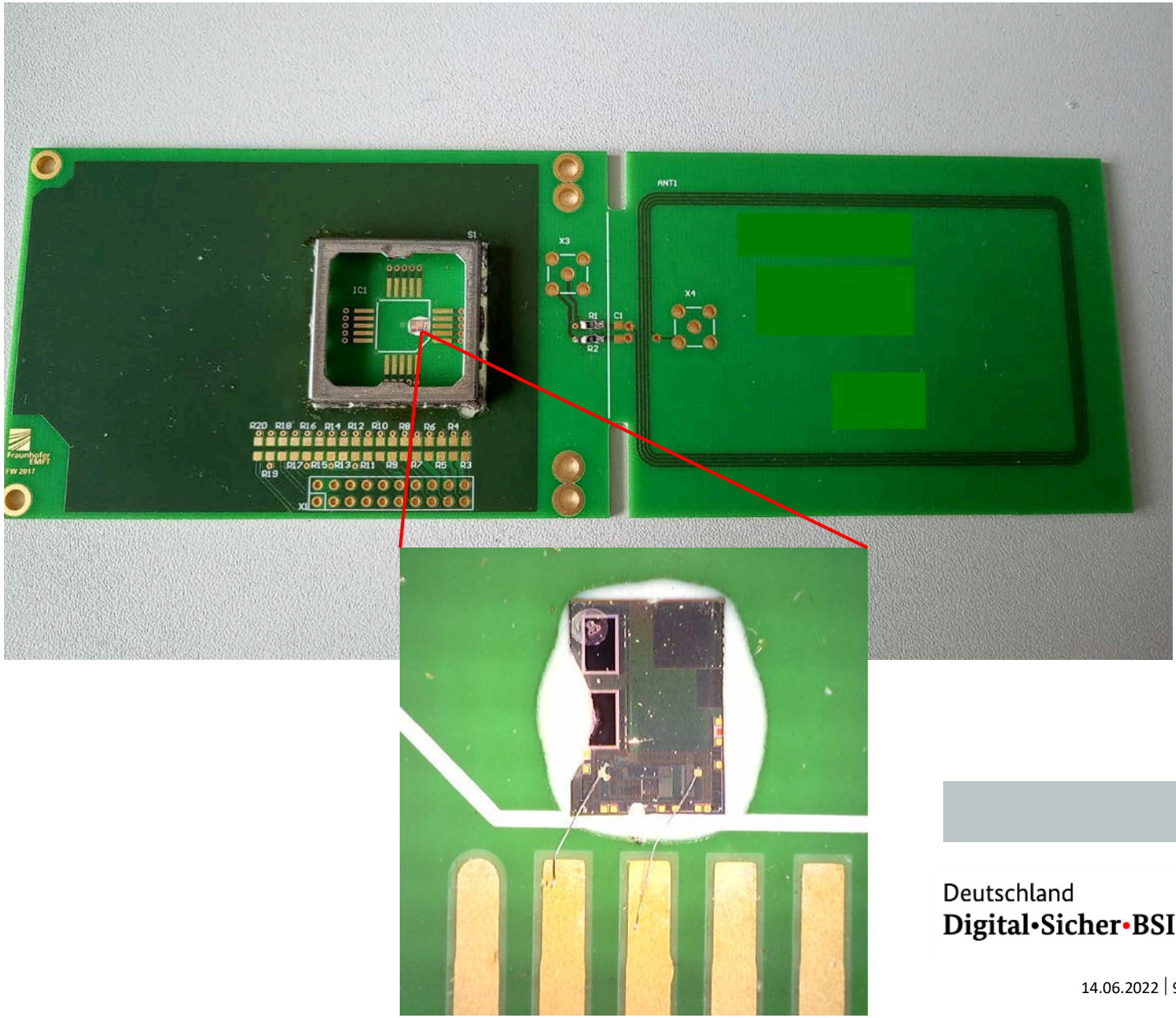
Präparationsschritte

- **Vergussmasse & Plastik**
- **Lösungsmittel**
- **Rauchende Salpetersäure**
- Metallseite: (Re)-Bonding
- Siliziumseite: Dünnen des Chips



Präparationsschritte

- Vergussmasse & Plastik
- Lösungsmittel
- Rauchende Salpetersäure
- **Metallseite: (Re)-Bonding**
- Siliziumseite: Dünnen des Chips

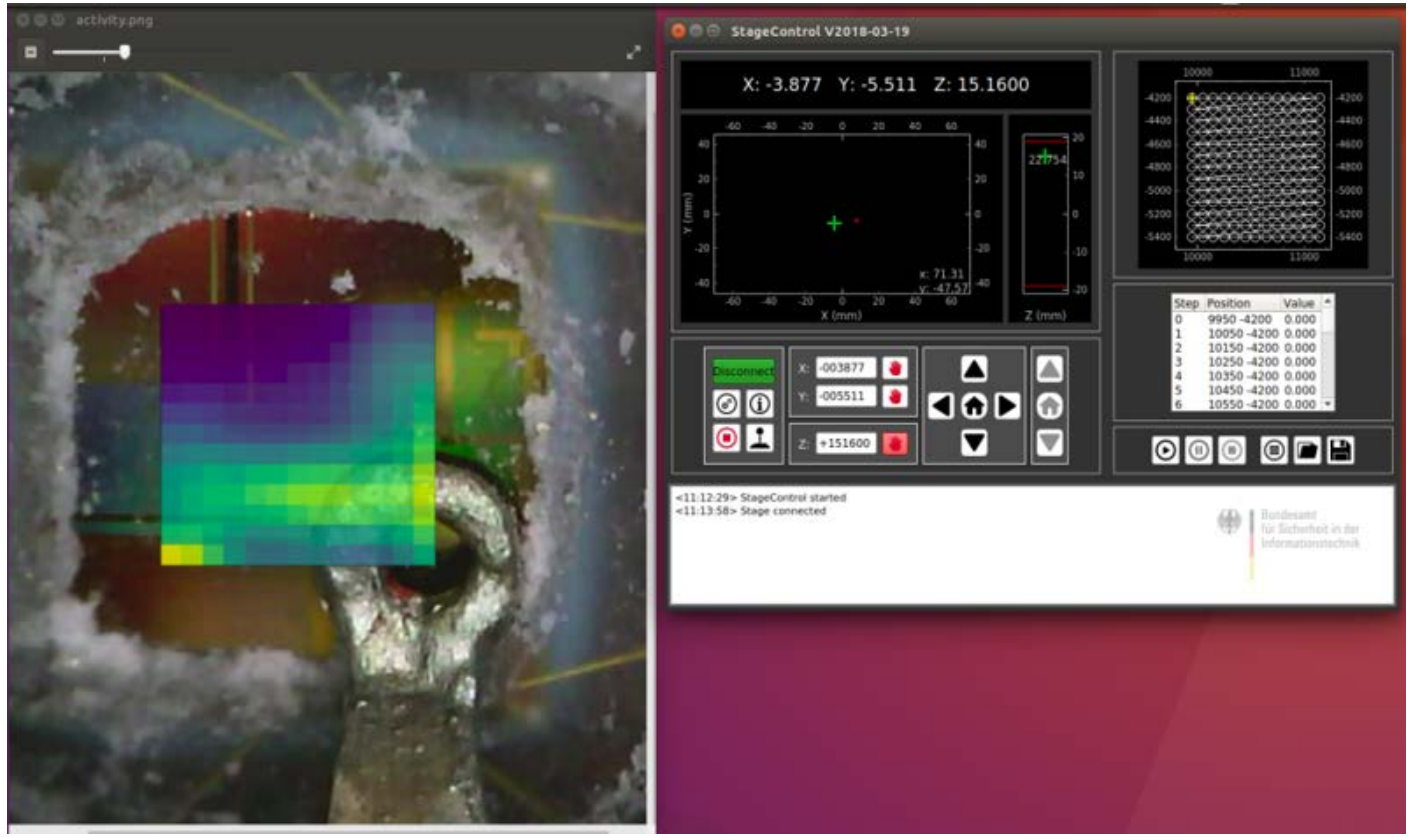


Präparationsschritte

- Vergussmasse & Plastik
- Lösungsmittel
- Rauchende Salpetersäure
- Metallseite: (Re)-Bonding
- **Siliziumseite: Dünnen des Chips**

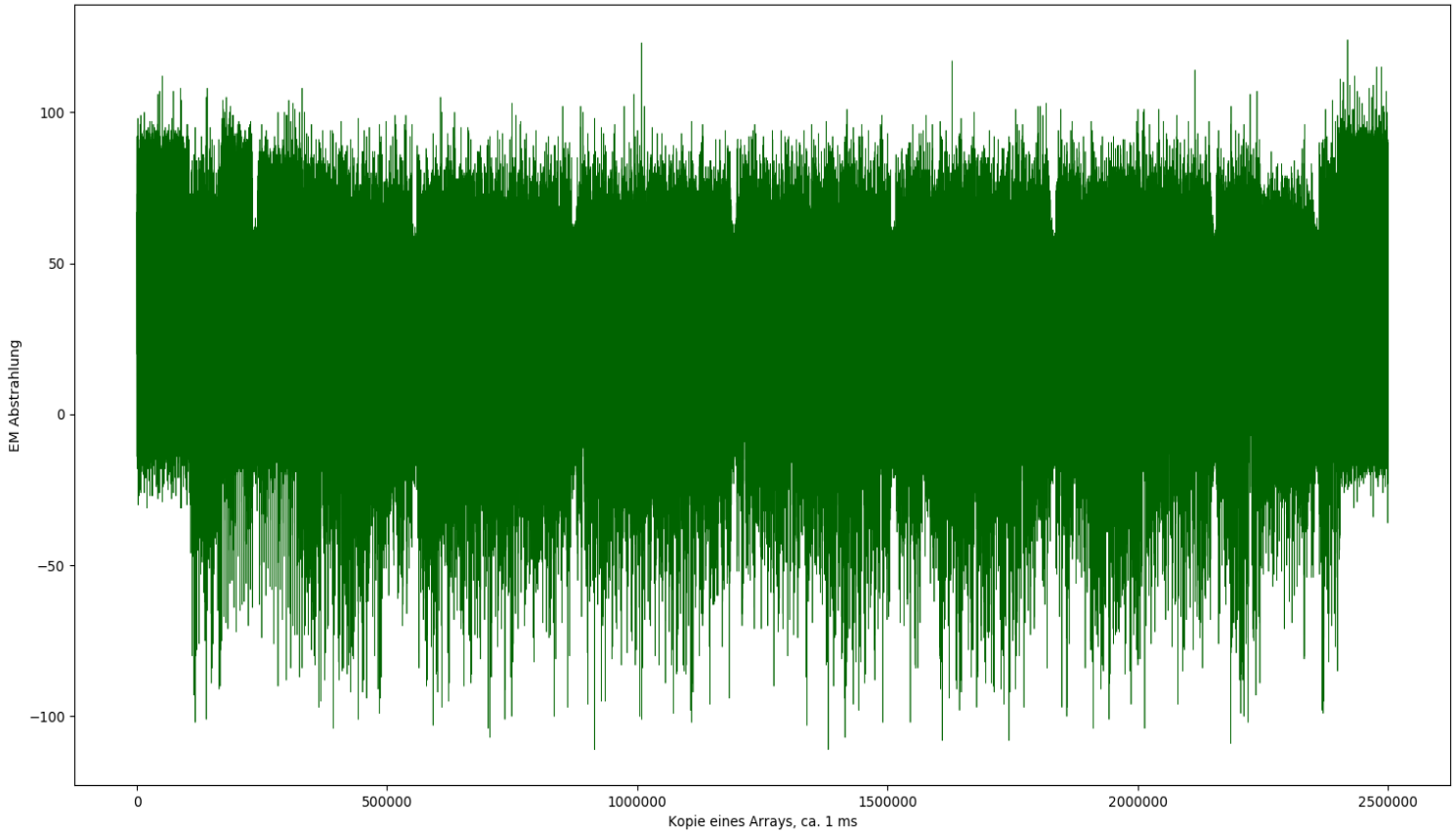
Leakage-Identifikation „Nadel im Heuhaufen“

- **örtlich: Wo auf dem Chip?**
  - **Metrik?**
- zeitlich: Wann kritische Berechnung?
- Big-Data
- eine Messung ~250 GB



Teil II: Theorie

- Daten- und Angriffsmodelle
- Schwierigkeiten
- klassische & KI-Verfahren
- Ausblick



Daten- und Angriffsmodelle

- gegeben: Seitenkanalmessungen („Traces“) + X
- X = zusätzliche Informationen, z.B. verwendete Hard/Software, Algorithmus, ggfs. implementieren Gegenmaßnahmen, zugehörige Daten (Plaintexte und Schlüssel),…
- Übergänge fließend, je nach Schutzbedarf/implementierten Sicherheitsmechanismen näher am schwarzen (z.B. Hochsicherheitschips) bzw. weißen Ende (z.B. IoT-Geräte)
  - für Sicherheitszertifizierungen: Worst-Case Adversary
  - in Praxis: irgendwo in der Grauzone

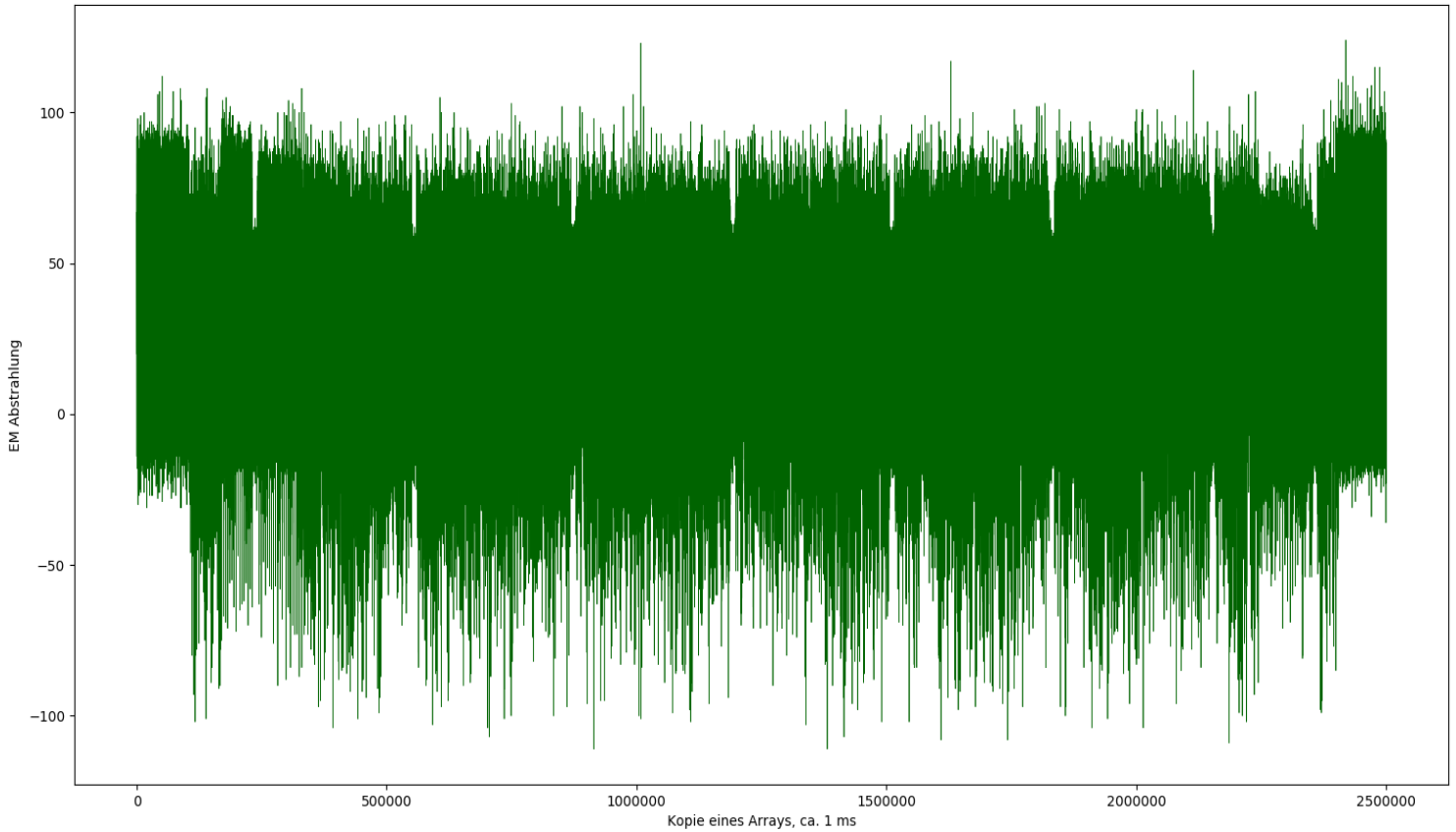
Blackbox
keinerlei weitere Informationen

Graybox
partielle Informationen, z.B. zu Implementierung, ggfs. baugleiches Trainingsgerät vorhanden

Whitebox
vollständige Information, inklusive Quellcode

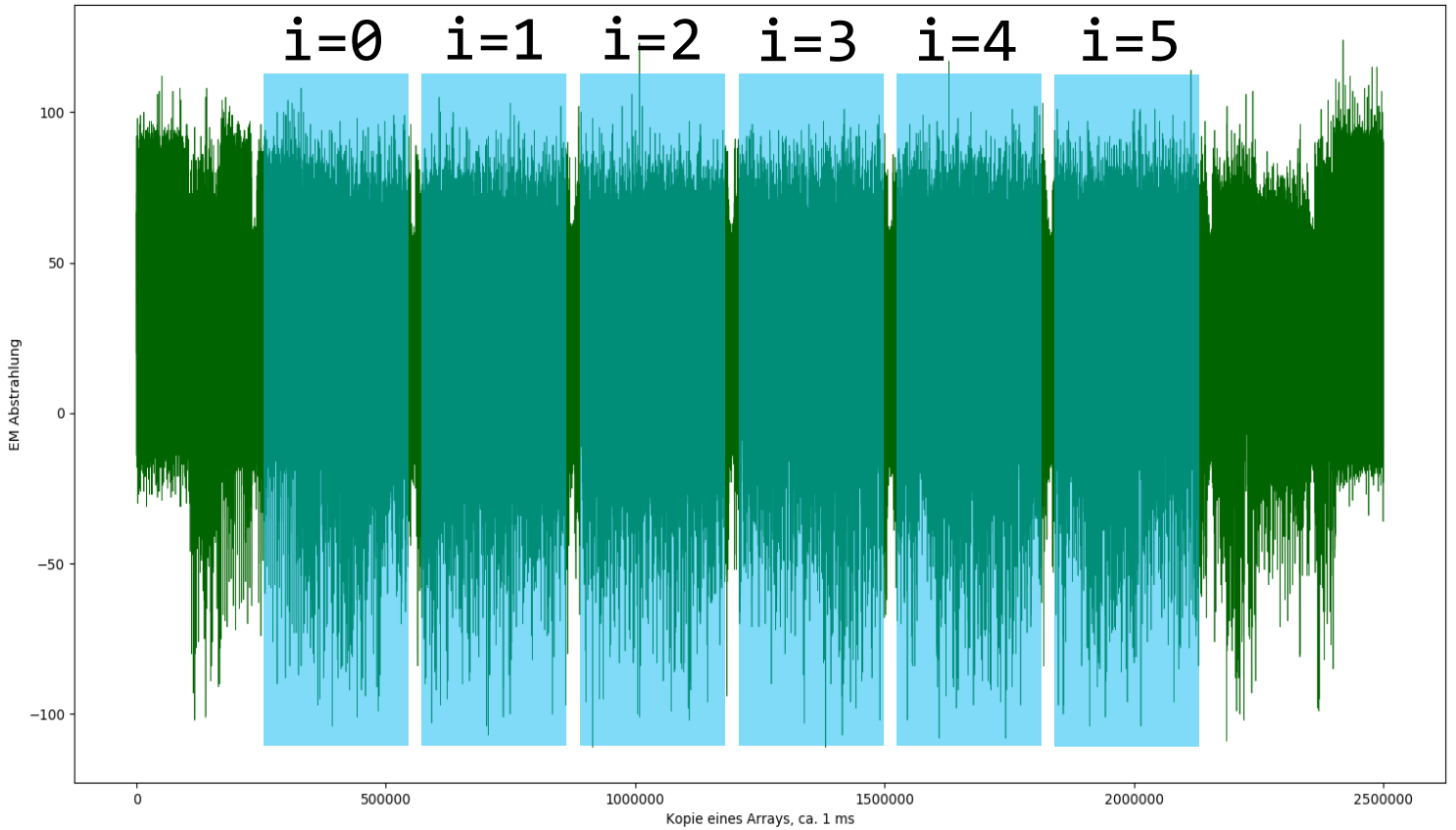
Blackbox-Modell

- extrahierbare Informationen:
  - Rückschlüsse auf Algorithmus (z.B. Rundenstruktur)
  - Rückschlüsse auf Operationen (z.B. Kopierroutinen/Schleifen)



Blackbox-Modell

- extrahierbare Informationen:
  - Rückschlüsse auf Algorithmus (z.B. **Rundenstruktur**)
  - Rückschlüsse auf Operationen (z.B. **Kopierroutinen/Schleifen**)

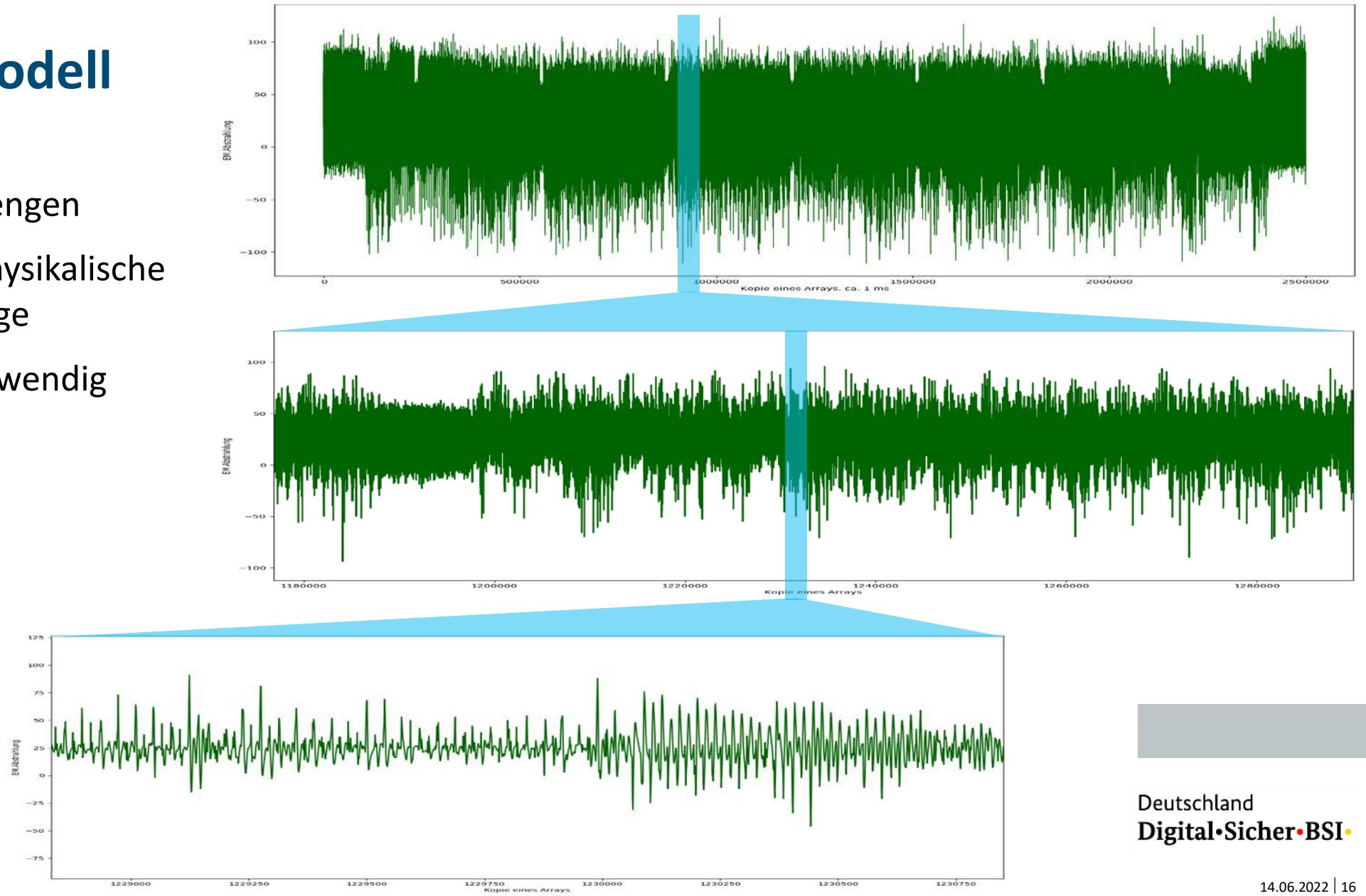



```
for(int i=0;i<6;i++) {
    dest[i] = source[i];
}
```

Graybox-Modell

- große Datenmengen
- komplizierte physikalische Zusammenhänge

-> **Reduktion** notwendig

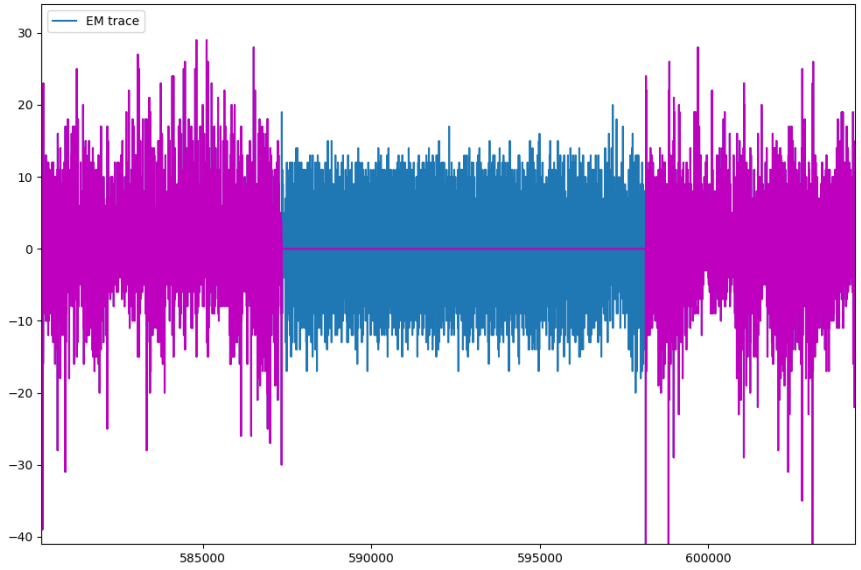


Schwierigkeiten und Problemreduktion

- **Komplexitätsreduktion**: Divide & Conquer-Strategie, Angriff von Teilgeheimnissen (z.B. einzelne Schlüsselbytes)
- **Datenreduktion**: Fokussierung auf einzelnen Operationen, Auswahl von Points of Interest (POI)
- vereinfachte **Leakagemodellierung**, z.B. Hamming-Weight Modell
- Umgang mit **Schwierigkeiten/Gegenmaßnahmen**, darunter:
  - Noise
  - Misalignment
  - Random Delay / Interrupts
  - Clock Jitter
  - Dummy-Runden
  - Masking

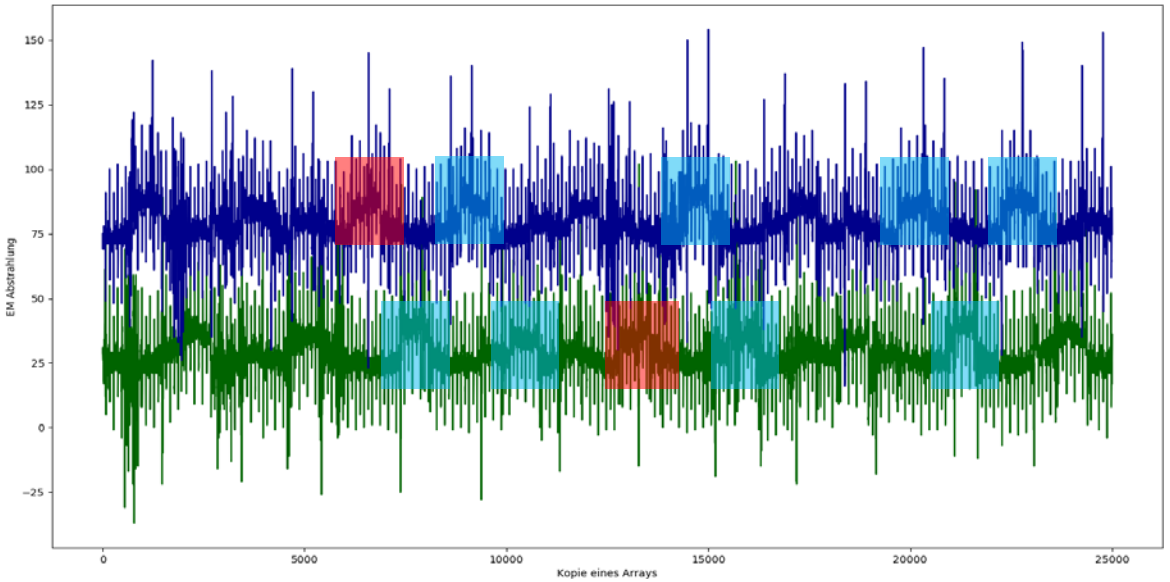
Schwierigkeiten und Problemreduktion

- Komplexitätsreduktion: Divide & Conquer-Strategie, Angriff von Teilgeheimnissen (z.B. einzelne Schlüsselbytes)
- Datenreduktion: Fokussierung auf einzelnen Operationen, Auswahl von Points of Interest (POI)
- vereinfachte Leakagemodellierung, z.B. Hamming-Weight Modell
- Umgang mit Schwierigkeiten/Gegenmaßnahmen, darunter:
  - Noise
  - Misalignment
  - **Random Delay / Interrupts**
  - Clock Jitter
  - Dummy-Runden
  - Masking



Schwierigkeiten und Problemreduktion

- Komplexitätsreduktion: Divide & Conquer-Strategie, Angriff von Teilgeheimnissen (z.B. einzelne Schlüsselbytes)
- Datenreduktion: Fokussierung auf einzelnen Operationen, Auswahl von Points of Interest (POI)
- vereinfachte Leakagemodellierung, z.B. Hamming-Weight Modell
- Umgang mit Schwierigkeiten/Gegenmaßnahmen, darunter:
  - Noise
  - Misalignment
  - Random Delay / Interrupts
  - Clock Jitter
  - **Dummy-Runden**
  - Masking

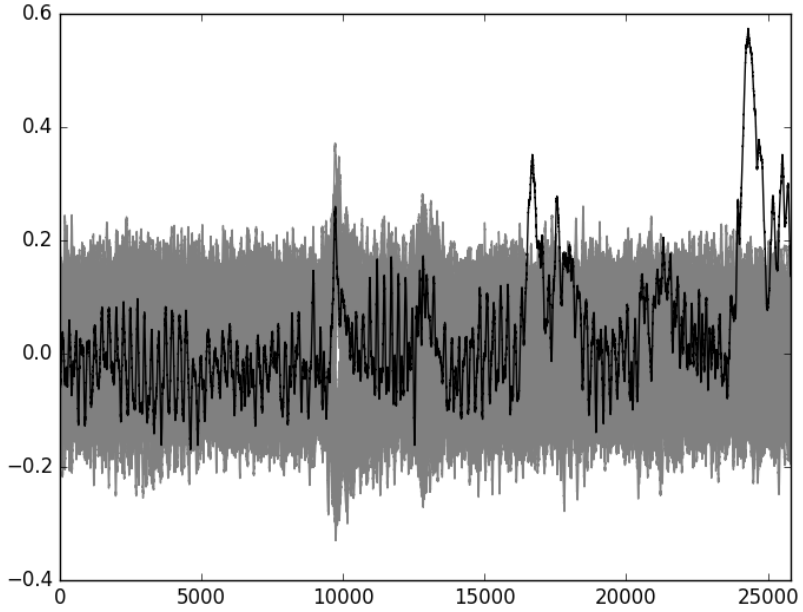


Graybox-Modell

- baugleiches Trainingsgerät und Trainingsdatensätze vorhanden?
  -> **profiled** vs. **non-profiled**
- **klassische, statistische Verfahren**:
  - Correlation Power Analysis (CPA, non-profiled)
  - Template Attacken
  - Stochastischer Ansatz
- **Machine Learning Verfahren („KI-Methoden“)**:
  - Support Vector Machines (SVMs)
  - Random Forests
  - Graphical Models
  - (tiefe) neuronale Netze

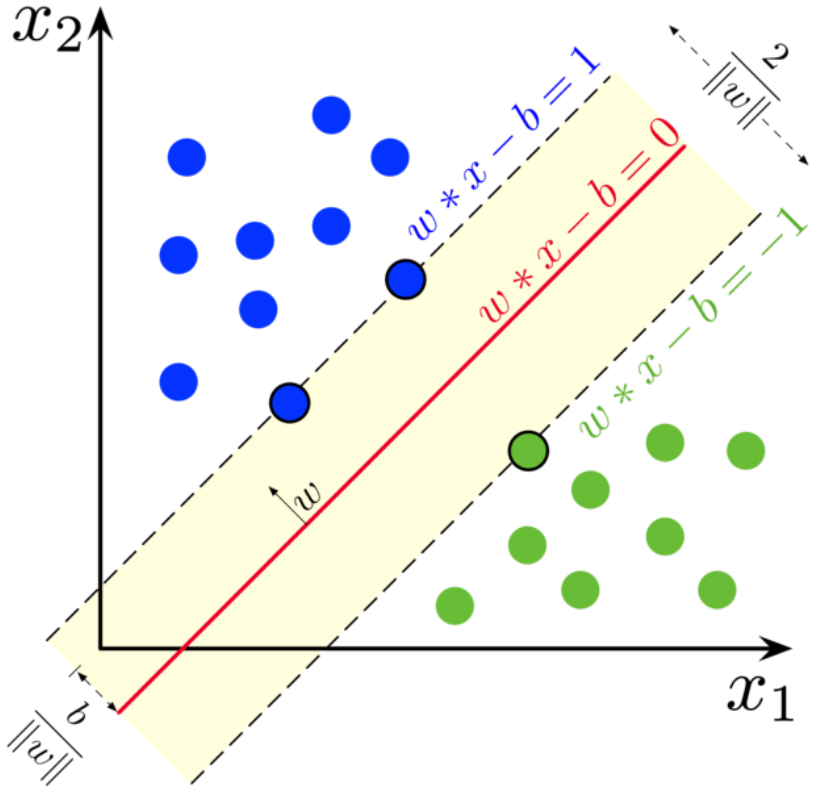
Graybox-Modell

- baugleiches Trainingsgerät und Trainingsdatensätze vorhanden?
  -> profiled vs. non-profiled
- klassische, statistische Verfahren:
  - **Correlation Power Analysis** (CPA, non-profiled)
  - Template Attacken
  - Stochastischer Ansatz
- Machine Learning Verfahren („KI-Methoden“):
  - Support Vector Machines (SVMs)
  - Random Forests
  - Graphical Models
  - (tiefe) neuronale Netze



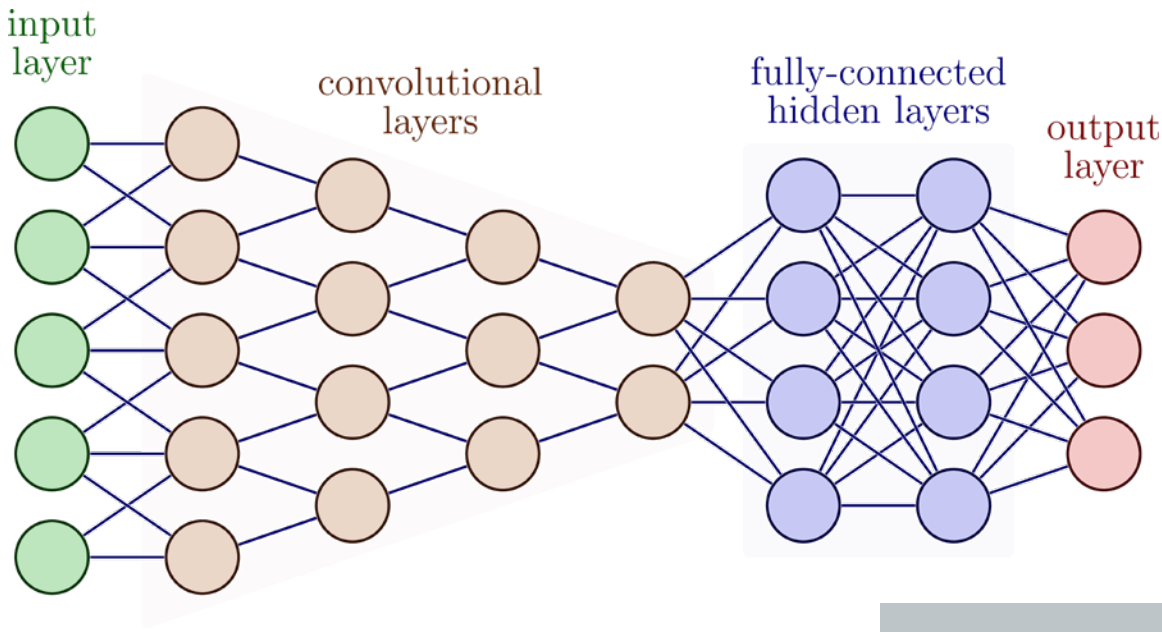
Graybox-Modell

- baugleiches Trainingsgerät und Trainingsdatensätze vorhanden?
  -> profiled vs. non-profiled
- klassische, statistische Verfahren:
  - Correlation Power Analysis (CPA, non-profiled)
  - Template Attacken
  - Stochastischer Ansatz
- Machine Learning Verfahren („KI-Methoden“):
  - **Support Vector Machines** (SVMs)
  - Random Forests
  - Graphical Models
  - (tiefe) neuronale Netze



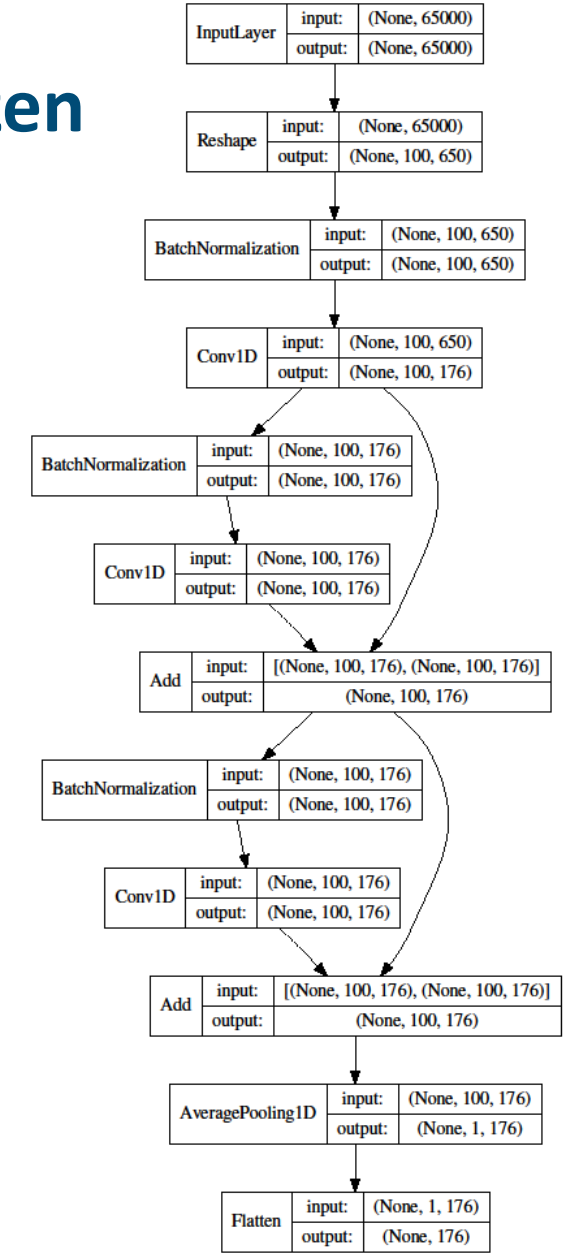
Graybox-Modell

- baugleiches Trainingsgerät und Trainingsdatensätze vorhanden?
  -> profiled vs. non-profiled
- klassische, statistische Verfahren:
  - Correlation Power Analysis (CPA, non-profiled)
  - Template Attacken
  - Stochastischer Ansatz
- Machine Learning Verfahren („KI-Methoden“):
  - Support Vector Machines (SVMs)
  - Random Forests
  - Graphical Models
  - **(tiefe) neuronale Netze**



Seitenkanalanalyse mit neuronalen Netzen

- keine POI-Auswahl nötig, Netz sucht sich Informationen selbst
- gewisse Robustheit gegenüber Gegenmaßnahmen wie Misalignment oder Masking
- Deep Learning Verfahren sind klassischen Verfahren teilweise deutlich überlegen
- weitere Forschung nötig, u.a. hinsichtlich Interpretierbarkeit, Leakage Detection
- Kombination klassischer und KI-basierter Verfahren möglich?



Zusammenfassung und Ausblick

- **Relevanz:** Seitenkanalangriffe sind von hohem Interesse für akademische Forschung und Industrie und spielen eine wichtige Rolle bei Sicherheitsevaluierungen
- **Interdisziplinarität:** Seitenkanalangriffe erfordern Kenntnisse aus Mathematik & Ingenieurswissenschaft
- aktuelle **Herausforderungen:**
  - Entwicklung und Einsatz von KI-Verfahren
  - Migration auf seitenkanalresistente PQC

Vielen Dank für Ihre Aufmerksamkeit!

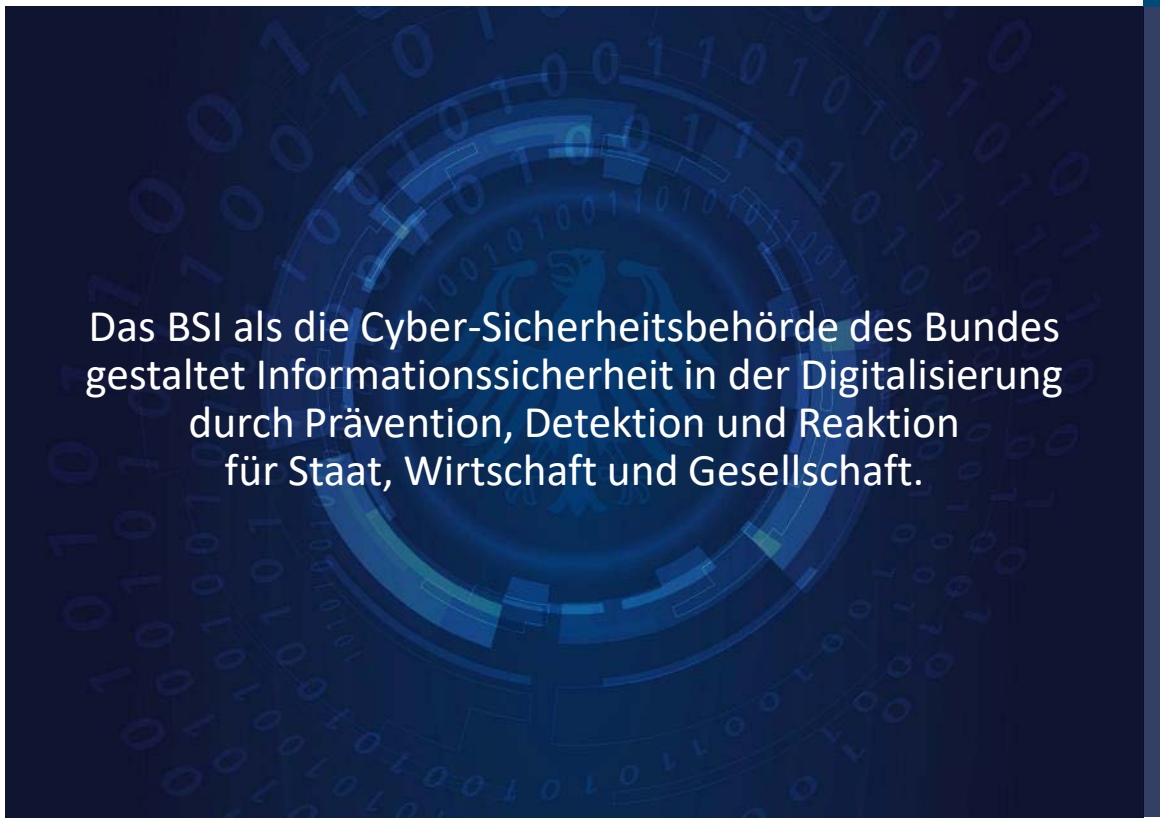
Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Dominik Klein (TK 11),
Dr. Friederike Laus (KM 22), Prof. Dr. Werner Schindler (RL KM 22)

vorname.name@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik