Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Trusted Electronics

More Trust, Better Platforms

1. Cybersicherheitstag, 9. November 2023, Fraunhofer AISEC

Introduction
Hardware Security Department

- **About us**
- 19 security researcher and 20+ students
- Dr. Matthias Hiller, head of department
- Dr. Nisha Jacob-Kabakci, head of PAC group

- **About me**
- Head of *Secure Processor Platforms* group
- Trusted electronics, RISC-V, open-source hardware
- 10 years security engineering and research

Architecture

- **Standard compliance**
- **Training courses**
- **Risk analysis**
- **Tamper protection**
- **New product design**
- **Guidelines & reference papers**

Implementation

- **Secure element ASIC**
- **Traditional and post-quantum cryptography**
- **Physical unclonable functions**

Laboratory

- **IC preparation**
- **Hardware pentesting**
- **IC analysis** (photonic emission)
- **Side-channel analysis**
- **Fault analysis** (laser, EM, glitching)

Motivation

What is trusted?[1]

1. High levels of quality and reliability.

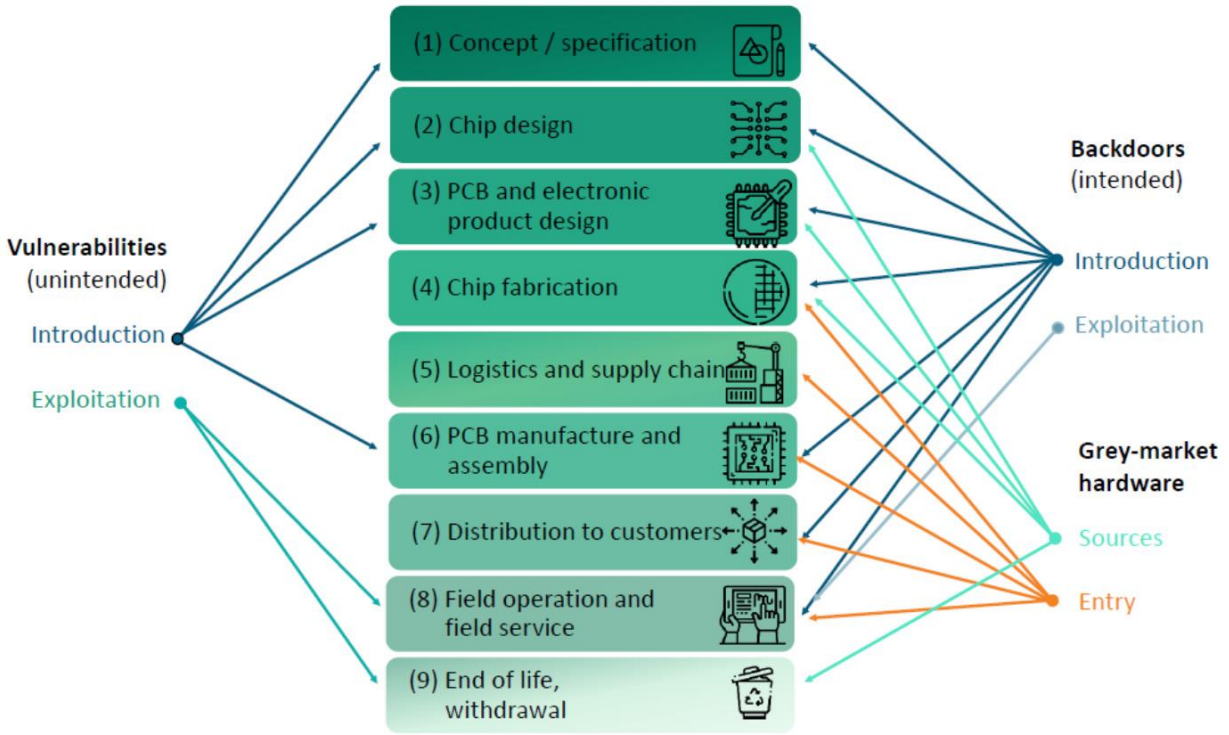
- Reliable operation of hardware in the field over its full lifetime.

2. Compliance to a known & complete specification.

- Functionality cannot be altered from the specification.

3. Hardened against state-of-the-art attacks.

- Mechanisms to ensure security and avoid vulnerabilities.



[1] VE-Velektronik reference paper: **DE** & **EN**
www.velektronik.de

Motivation

Open-source Hardware

- **Links to trusted electronics**
- Accessibility fosters innovation and competition (1)
- Transparency enables traceability (2)
- Community drives bug hunting (3)

- **Our objectives**
- Fraunhofer *next generation computing* agenda [1]
- Relevant and visible research vehicles
- Increased value creation for public funding

RISC-V ⇏ Open-source

[1] https://www.fraunhofer.de/en/research/fraunhofer-strategic-research-fields.html

Motivation

Project Landscape

- **VE-Velektronik** [1]
- BMBF project as part of ZEUS [2] call
- 2021 – 2024, 15 partner (Fraunhofer, Leibnitz, edacentrum)
- Reference paper on trusted electronics
  - Unintentional bugs in early design steps
  - Grey market hardware (overproduction, use of rejects)
  - Intentional manipulation in late value chain steps
- **Study for EU commission upcoming!**

- **Bavarian funding initiatives (85+ Mio. €)**
- **Trusted Electronic Bayern Center** (TrEB) [3]
  - Hardware and system designs at IoT level
  - Expansion of hardware security analysis laboratories
- **Bayerisches Chip-Design-Center** (BCDC) [4]
  - Education and reduction of talent shortage
  - Portfolio of hardware designs incl. ecosystem
  - Accessibility to (low-volume) IC production

Gefördert durch
Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

[1] https://www.velektronik.de
[2] https://www.elektronikforschung.de/foerderung/bekanntmachungen/zeus
[3] https://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/pressemitteilungen/2022/mikroelektronik-forschung-in-bayern.html
[4] https://www.iis.fraunhofer.de/de/ff/sse/bayerisches-chip-design-center.html

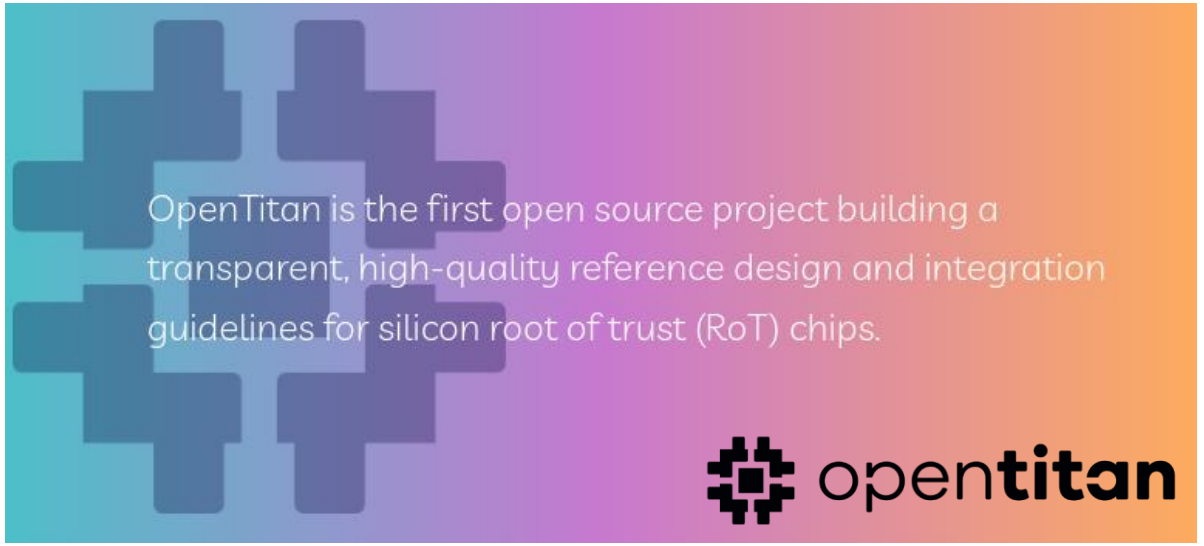
OpenTitan Project

Overview

- **OpenTitan project [1,2]**
- lowRISC, Google, ETH Zürich, G+D, Nuvoton, …
- System-on-chip (SoC) for authentication and platform integrity
- µC range: Ibex 32-bit (“zero-riscy”) RISC-V core

- **Our motivation**
- Research on a *real-world,* security-focused µC platform
- Increasing accessibility to secure and affordable hardware

- **Our relation to the project**
- Project user since end of 2019
- Not part of the consortium

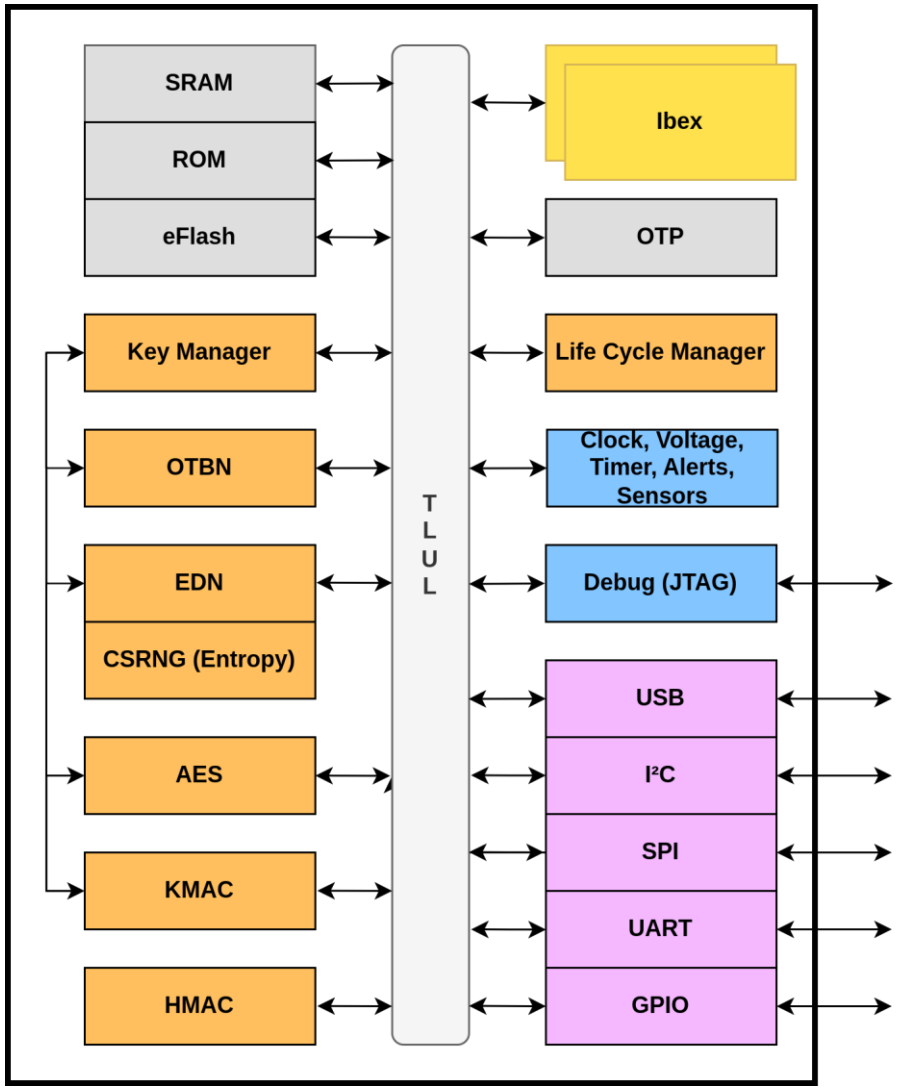


[1] https://opentitan.org/
[2] https://github.com/lowRISC/opentitan

OpenTitan Project
Properties

- ***Earl Grey* top-level design** [1]
- 100 MHz, 32-bit, 3-stage, dual-core lockstep CPU
- eFlash, SRAM, ROM, OTP (all scrambled)
- AES, SHA-2/3, RSA, ECC, CSRNG (with selected countermeasures)
- Lifecycles, key manager, attestation, secure boot & update

- **Use-cases** [2]
- Platform integrity module
- Trusted platform module
- Universal 2nd-factor security key



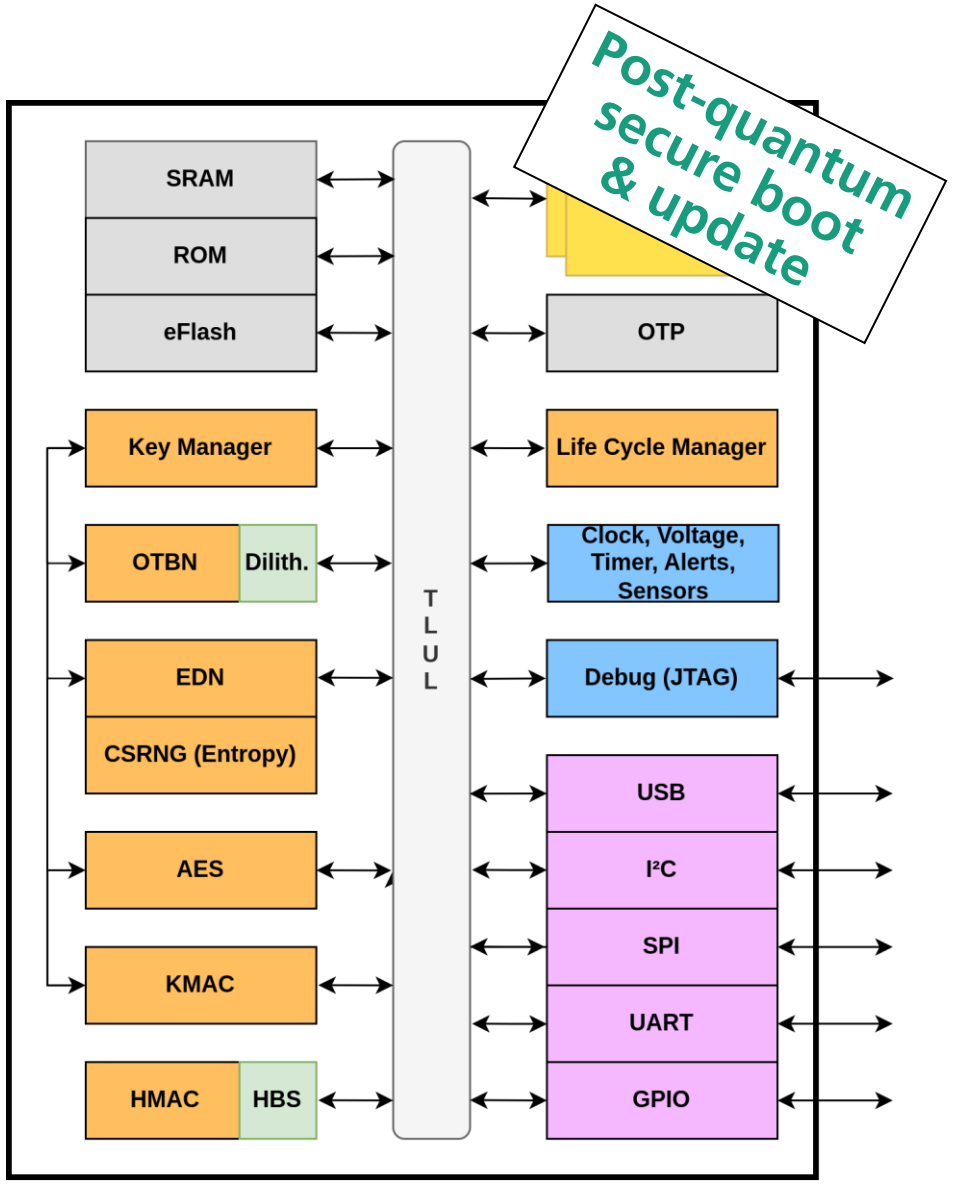
[1] https://opentitan.org/book/hw/top_earlgrey/doc/specification.html
[2] https://opentitan.org/book/doc/use_cases/index.html

OpenTitan Project

Extensions

- **Hash-based signature extension to HMAC / SHA-2 core** [1]
- LMS, XMSS, SPHINCS+
- 56 kGE (HMAC) + 11 kGE (LMS) + 6 kGE (SPX⁺-s)
- Signature size **1.6 kB** (LMS) and **29 kB** (SPX⁺-s)
- Public key size **32 bytes** (LMS) and **64 bytes** (SPX⁺-s)
- Signature verification in **10 ms** (LMS) and **50 ms** (SPX⁺-s)

- **CRYSTALS-Dilithium extension to OTBN** [2]
- Instruction set extensions for polynomial arithmetic and sampling
- 4711 kGE (OpenTitan) + 242 kGE (Dilithium)
- Signature size **4.6 kB**, public key size **2.6 kB**
- Signature verification in **22 ms**

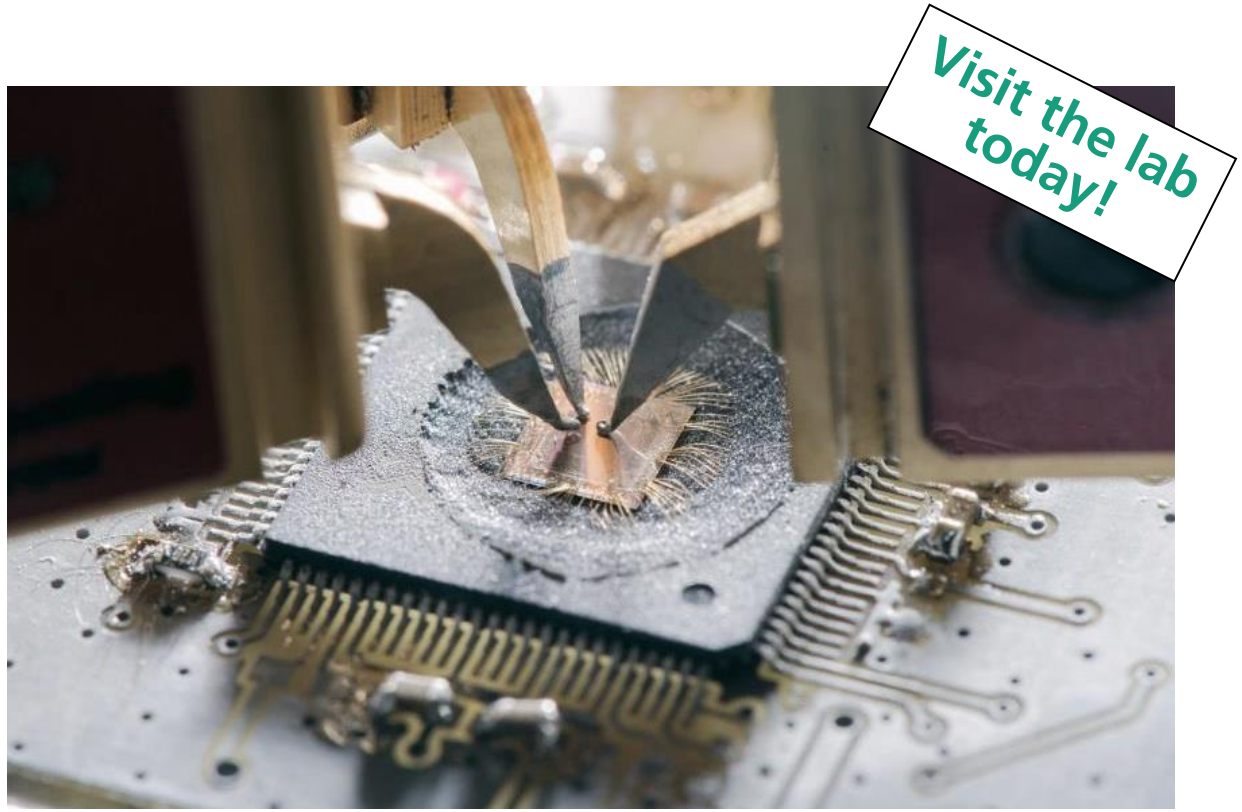


[1] A. Wagner, F. Oberhansl, M. Schink: https://doi.org/10.1145/3560834.3563831
[2] T. Stelzer, F. Oberhansl, J. Schupp, P. Karl: Accepted at ASHES 2023, 30. November, Copenhagen, http://ashesworkshop.org/

Security Assessment

Analysis in the Laboratory

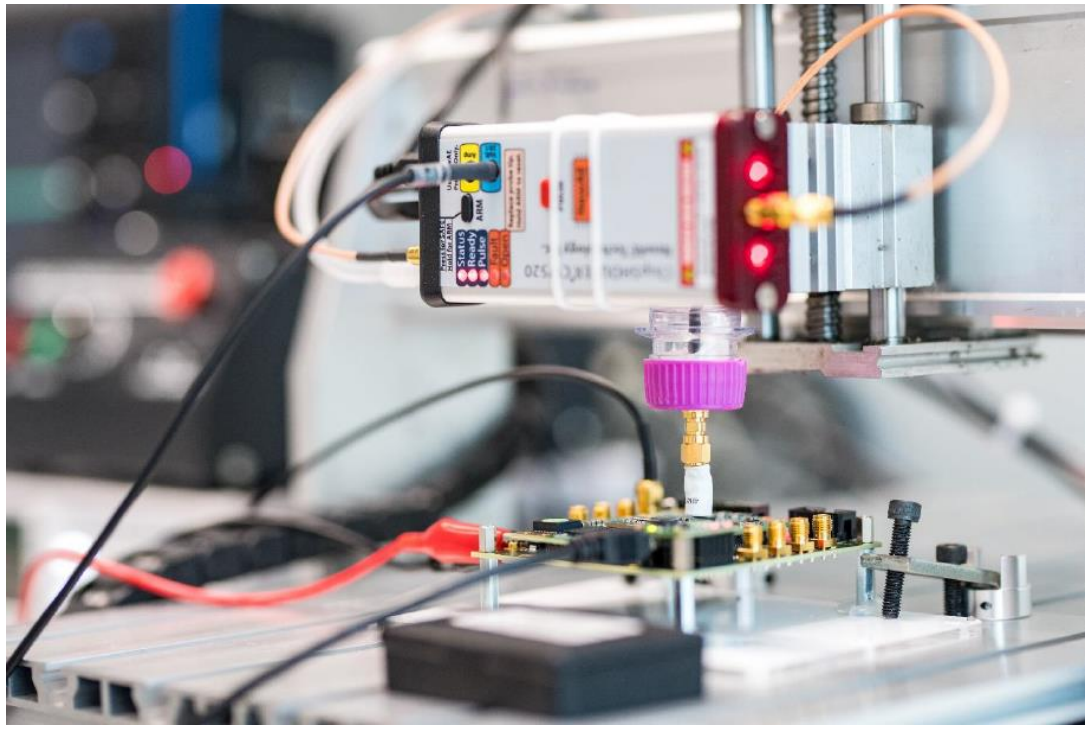
- **Analysis at AISEC**
- Power- and EM-based side-channel analysis
- Fault injection: laser, EM, glitching
- Invasive IC analysis
  - Decapsulation, etching
  - Electro Optical Probing (EOP)
  - Thermal laser stimulation (TLS)
- **Analysis at FhG**
- Advanced decapsulation, etching, delayering
- Advanced imaging capabilities
  e.g., scanning electron microscopy
- **Common Criteria site-certification ongoing**



Security Assessment

Hardware Attacks against µC

- ***Study on Hardware Attacks against Microcontrollers*** [1]
- On behalf of the German Federal Office for Information Security (BSI)
- **µC in security-relevant products**
- Hardware security keys
- Hardware crypto wallets
- Smart locks
- Point-of-sales terminals
- **Threats from:** supply chain, evil maid, device theft
- **Attacks** (control-flow manipulation, side-channel analysis, read-out protection bypass) and **countermeasures** (check out the study!)



[1] M. Schink, F. Oberhansl, A. Wagner, K. Zinnecker, A. Garcia: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/Hardware-Angriffe/Hardware-Angriffe_node.html

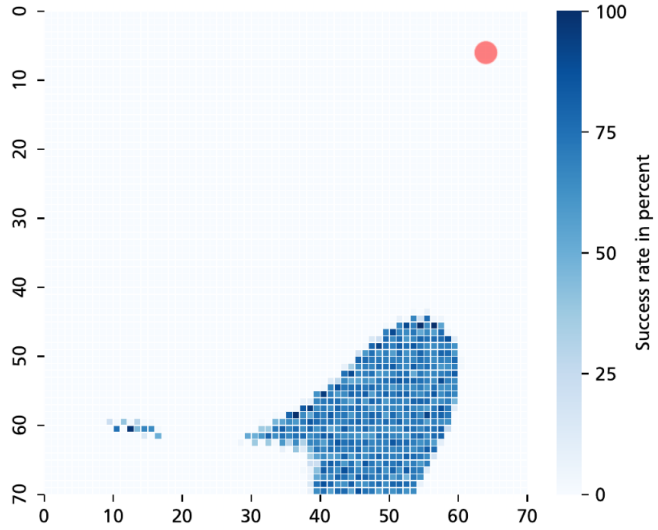
Security Assessment
Findings

- **Successful attacks**

- Debug unlock with flash erase suppression possible with EM fault injection → check for blank flash or sense EM pulses
- Secure boot bypass with single-instruction-skip through EM fault injection (MCUboot and mbedTLS) → redundant execution

- **Status Quo**

- Many security-relevant products are built based on COTS µC with no focus on security or no certification
- Lack of
  - … support for developers
  - … security documentation
  - … thorough reviews and testing



Fraunhofer AISEC

Conclusion

What's now, what's next?

- **Increased trust in electronics**
- Complex and international value chain
- RISC-V and open-source hardware can help
- It's a joint effort, so feel free to get in touch

- **New collaborative platforms?**
- Shared effort and shared cost
- Adequate and affordable security
- Broad application → high impact

- **Tag der vertrauenswürdigen Elektronik (TdvE)**
- 04. and 05. June 2024, Munich
- Connecting science, industry, government
- Organized by Fraunhofer EMFT and AISEC

- **Trusted Chips Kick-off [1]**
- 13. November 2023, Frankfurt & online
- Standardization needs & recommendations
- Coordinated by DKE, funded by EU

[1] https://www.dke.de/en/veranstaltungs-detailseite?id=22221&type=vde%7Cvdb

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Thank you for your attention

Andreas Seelos-Zankl
Head of Research Group
Secure Processor Platforms
Hardware Security Department
andreas.zankl@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Lichtenbergstraße 11
85748 Garching
www.aisec.fraunhofer.de