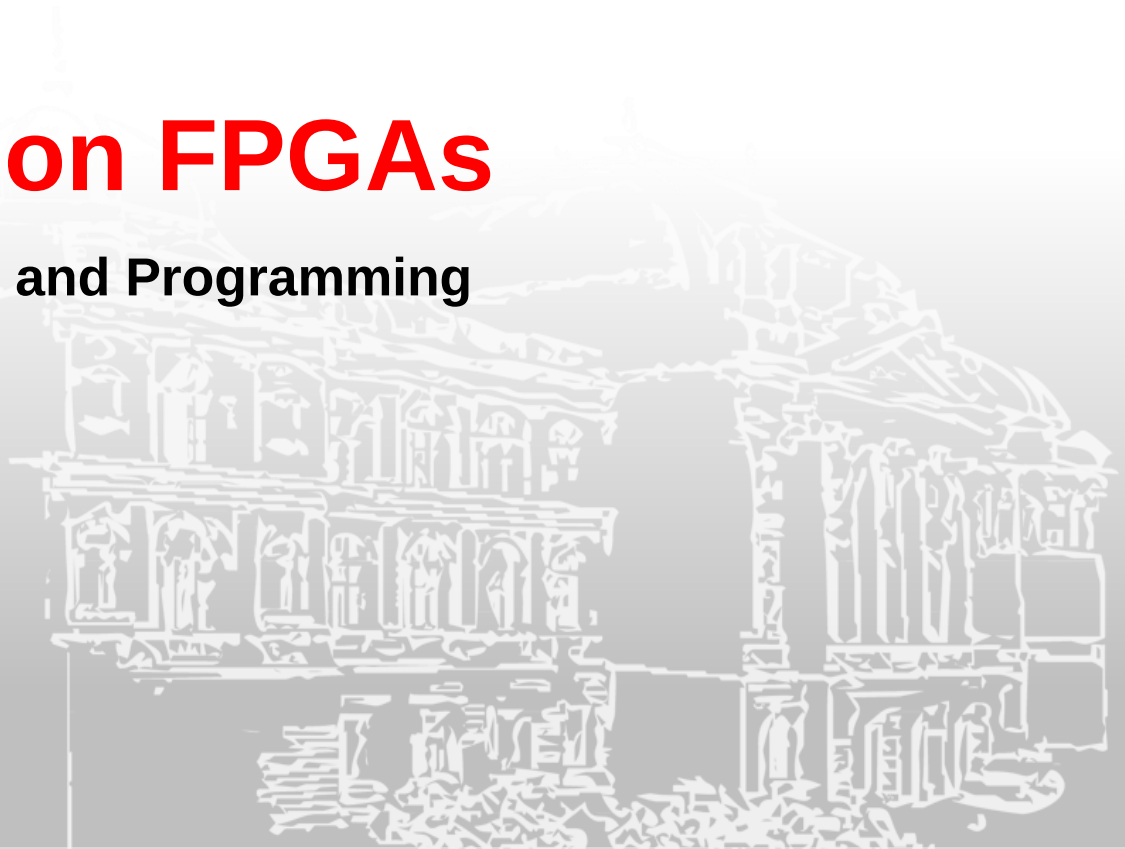
Fault Attacks on FPGAs

Digital System Integration and Programming

Lukas Furtner

14.12.2022



Agenda

- Fault Attacks in General
- Fault Attacks on FPGAs
- Conclusion/Comparison
- References

Fault Attacks in General

Fault Attacks

- Physical attack
  - Attack on hardware's properties [1]
  - Attack model: the attacker has access to the device
- Intentionally change device's operating condition
  - Various attack vectors (power, temperature …)
- Unintended behavior of the system can happen
  - Bit flips
  - Different timing behavior of hardware

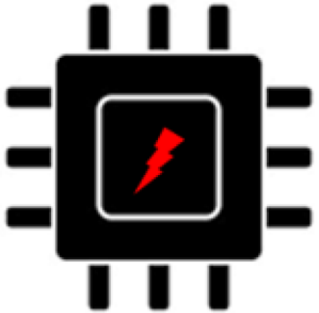


Fig. 1: Abstract fault on Chip

Fault Attacks

- Invasive method
  - Property of destruction
  - Chip modification
  - Chip suffers damage

- Non-invasive method
  - Do not damage the system
  - Not traceable

Fault Attacks

- Main attack vectors [1]
  - Voltage spikes
    - CMOS propagation delay is voltage dependent
    - Lower voltage, higher switching time $T_d \propto \frac{1}{V}$
  - Temperature
    - Higher temperature
      - Lower impedance for CMOS-channels
      - Higher impedance for transmission lines

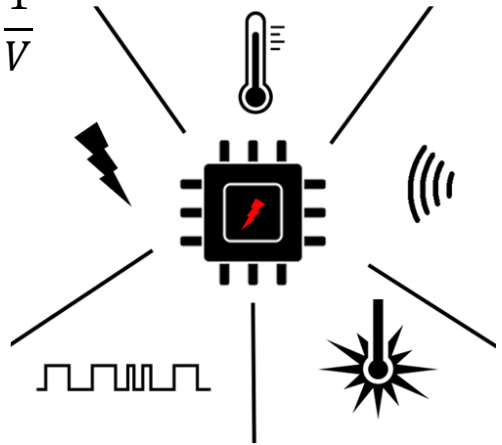


Fig. 2: Types of faults

Fault Attacks

- Main attack vectors [1]
  - Electromagnetic injection
    - Principle of induction
    - Flipping transistors
  - Laser injection
    - Ionization, Heating through Laser [2]
  - Clock glitching
    - Only with external clock sources
    - Create state transition when calculation is not finished

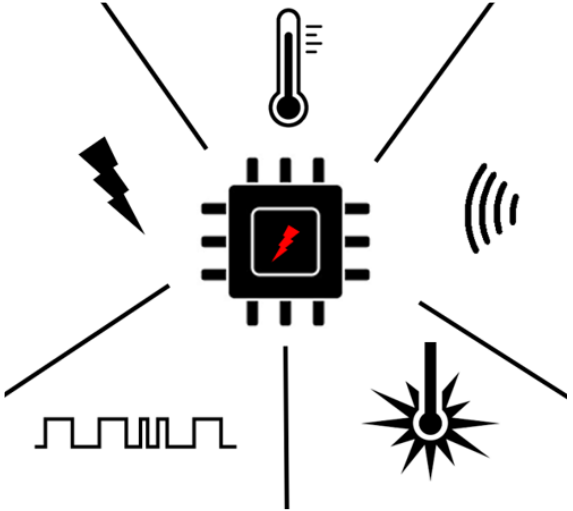


Fig. 3: Types of faults

Fault Attacks

- Effects of successful fault attack [1]
  - System changes behavior
    - Reveals sensitive data
    - Faulty computations
      - Broken systems
      - Wrong AI
      - Key recovery
    - System crashes

Fig. 4: PC on fire [3]

Fault Attacks on FPGAs

Fault Attacks on FPGAs

- FPGA's also use CMOS technology
- Similar attack vectors
- Most attractive attack
  - Voltage-Drop based faults
    - Ring oscillators
- Other existing attacks based on
  - Thermal laser stimulation
    - Seebeck voltage on Drain of MOSFET
  - Clock glitch attack

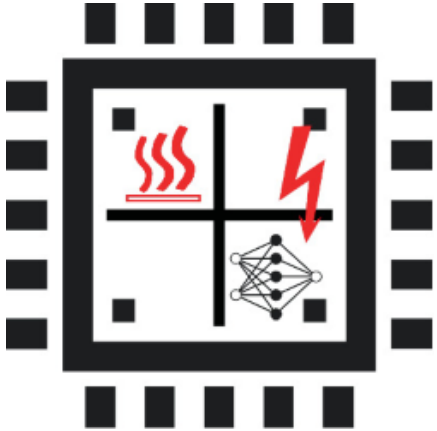


Fig. 5: Fault attack on chip [4]

Performed Fault Attacks on FPGAs

Two different performed attacks:

- First one based on voltage spike
- Second one based on Thermal Laser Stimulation

Remote and Stealthy Fault Attack on Virtualized FPGA

Lukas Furtner
14.12.2022

Key Informations

- Voltage based attack
- Executed on multi tenant FPGA
- FPGA-AES attacked
  - Key recovery attack
- Introduced timing faults
  - Between AES rounds
- DFA (Differential Fault Analysis used for key recovery)

Threat Model [5]

- Multi tenant FPGA
  - Attacker and victim on same board
- Logical isolation between
- Shared power supply

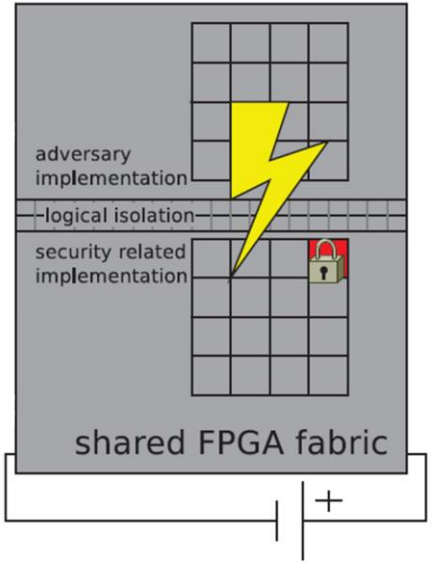


Fig. 6: Threat model 1 [5]

Attack

- Attacker FPGA stream consists of many ring oscillators [5]
- Turn them on at the same time
  - Ring oscillators need a lot of power to be driven
  - If enough ring oscillators
    - Voltage dip on power rail
- Usually 30-50% of the FPGA needed for big enough voltage dip

Attack

- Voltage dip leads to higher transmission [5]
  - AES combinatoric logic does not finish
  - Next state transition introduces faulty state
  - State propagated through scheme
  - Different outputs for correct and faulty value
    - DFA possible

$$T_d \propto \frac{1}{V}$$

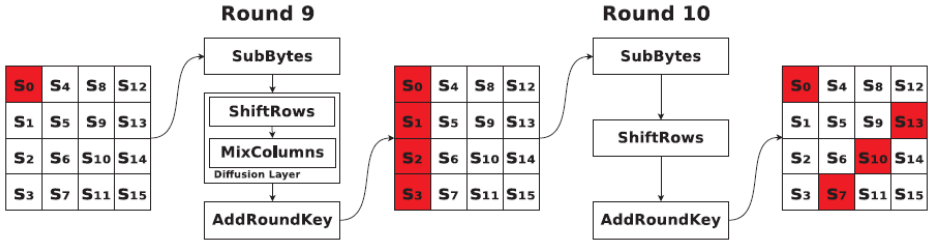


Fig. 7: AES fault propagation [5]

How well does it work

- Very successful attack
- On different FPGAs [6]

- Benchmark IPs also very good for voltage dip attack [6]

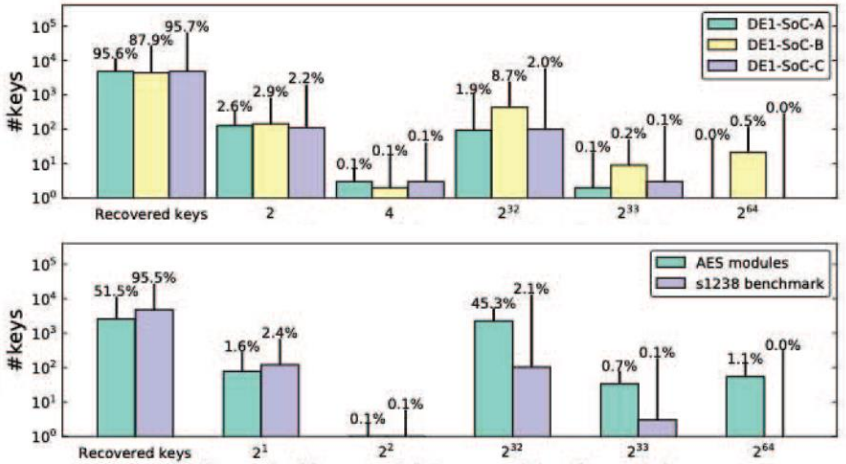


Fig. 8: Success rate of attack (remaining key candidate numbers of 5000 keys [6]

Countermeasures

- Hard to implement [6]
  - Search bitstream for ring oscillators
    - Attack also possible with multiple AES/Benchmark IP-cores

- Better:
  - Search for power intense parts [6]
    - Use separate power rails for them
      - Multi tenant system needs to support that

Key Extraction Using Thermal Laser Stimulation

Lukas Furtner
14.12.2022

Key Informations

- Laser Injection based attack
- Executed on physical accessible FPGA
- FPGA-battery-backed SRAM attacked (BBRAM)
  - AES key of bitstream stored in there
    - Used for decrypting bitstream from non-volatile memory during startup
- Introduced thermal heating on BBRAM-MOSFETs drain
  - Generates voltage (seebeck-voltage)
  - Can be measured on supply line

Threat Model [2]

- Physical access to the FPGA
- Attacker owns an FPGA of the same type
- Attacker can have but does not need access to the floorplan of the chip

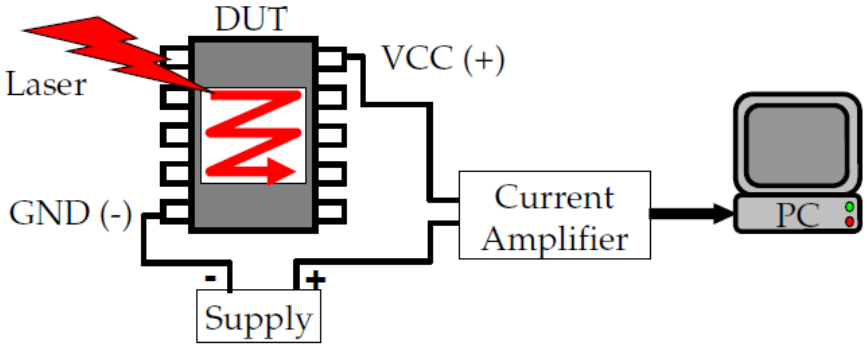


Fig. 9: Threat model 2 [2]

Attack

- Laser beam used to heat drain of MOSFET [7]
  - Temperature gradient
  - Two different metals
    - Diffusion of carriers
    - Seebeck voltage

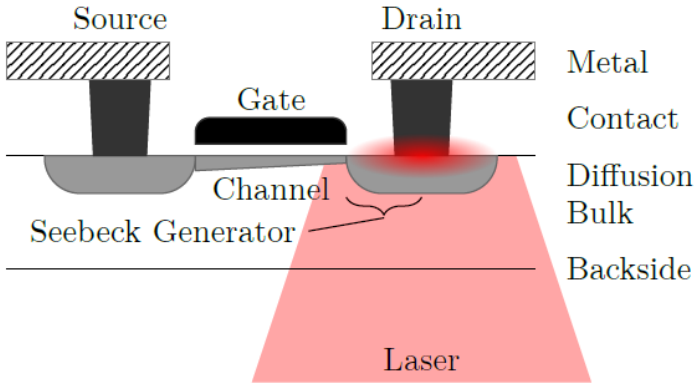


Fig. 10: Introducing Seebeck voltage with Laser [7]

What can be done with that

- SRAM cells
  - Heating MOSFET drain [7]
    - Opposite MOSFET opens a bit (still very high ohmic)
      - Current change on power rail [nA]
    - Only applies for closed connection
      - Active MOSFETs
- Differentiate between 0 and 1 bit

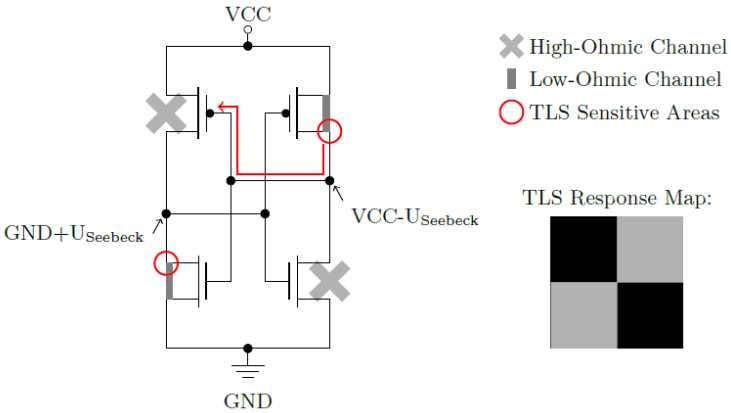


Fig. 11: SRAM bit recovery [7]

FPGAs use BBRAM

- Battery-Backed-SRAM
  - SRAM format can be attacked [8]
  - Battery backed
    - Low noice - better detection of small currents
- 2D-Map of laser stimulation created [8]
- Reference with 0 bits
- Create difference

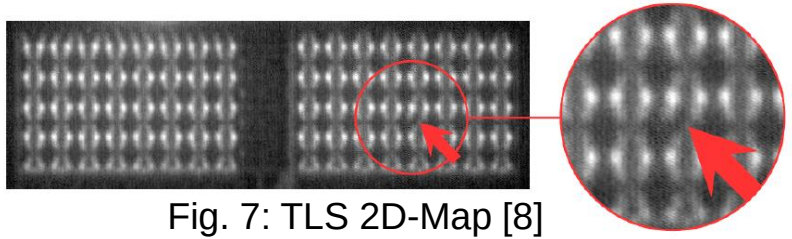


Fig. 7: TLS 2D-Map [8]

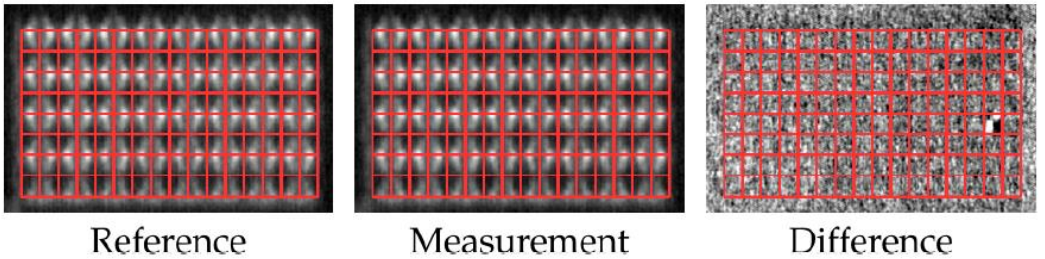


Fig. 12: Difference of TLS 2D-Map [8]

Extendable for Whole Key

- Apply threshold for black and white parts [8]
- Cells with black and white
  - Indicate difference to 0 bit
    - Contain a 1

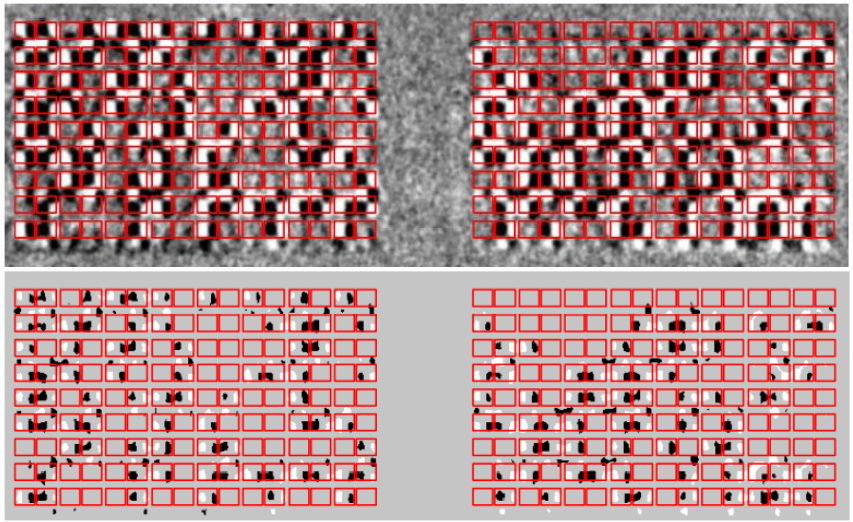


Fig. 13: Whole Key Recovery [8]

Countermeasures

- Noice based countermeasure [8]
  - More measurements reduce SNR
- Light sensors useless
  - To long wavelength
- Temperature sensor would work
  - Battery driven, because attack performed during shut down
- Bit obfuscation by hardware [8]
  - Works, but duplication of circuit still possible
  - Could be revealed at a later point

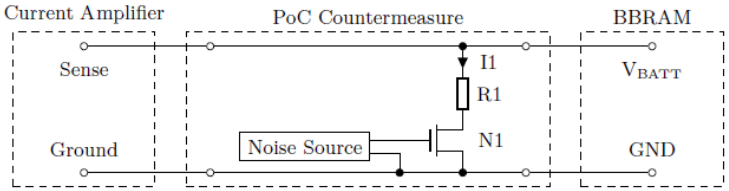


Fig 14: Noice based countermeasure circuit [8]

Comparison of Attacks

First attack

- Attack vector
  - Voltage dips
- Attack on
  - FPGA calculation
- Remote attack
- Relatively easy

Second attack

- Attack vector
  - Thermal Laser Stimulation
- Attack on
  - BBRAM
- Access to device needed
- Expensive equipment

References and Image Sources

- [1] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," in Proceedings of the IEEE, vol. 94, no. 2, pp. 370-382, Feb. 2006, doi: 10.1109/JPROC.2005.862424.
- [2] F Beaudoin, R Desplats, P Perdu, and D Lewis. Implementing thermal laser stimulation in a failure analysis laboratory. In International Symposium for Testing and Failure Analysis, pages 151–160. ASM International, 2001.
- [3] unknown. (2022). https://upload.wikimedia.org/wikipedia/en/f/f2/Computer_on_fire.svg
- [4] Tajik, Shahin & Ganji, Fatemeh. (2020). Artificial Neural Networks and Fault Injection Attacks.

References and Image Sources

- [5] J. Krautter, D. R. E. Gnad, and M. B. Tahoori, “FPGAhammer: remote voltage fault attacks on shared FPGAs, suitable for DFA on AES,” IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), vol. 2018, no. 3, 2018.

- [6] J. Krautter, D. R. E. Gnad and M. B. Tahoori, "Remote and Stealthy Fault Attacks on Virtualized FPGAs," *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021, pp. 1632-1637, doi: 10.23919/DATE51398.2021.9474140.

- [7] Christian Boit, Clemens Helfmeier, Dmitry Nedospasov, and Alexander Fox. Ultra high precision circuit diagnosis through seebeck generation and charge monitoring. In *Physical and Failure Analysis of Integrated Circuits (IPFA), 2013 20th IEEE International Symposium on the*, pages 17–21. IEEE, 2013.

- [8] Lohrke, H., Tajik, S., Krachenfels, T., Boit, C., & Seifert, J.-P. (2018). Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2018*(3), 573–595. https://doi.org/10.13154/tches.v2018.i3.573-595

Fault Attacks on FPGAs

Digital System Integration and Programming

Lukas Furtner

14.12.2022