Fault Attacks on FPGAs

Florian Berger

November 29, 2023

Outline

Introduction to Fault Attacks

Case Study: Remote PDN Fault Attacks

Case Study: Local Thermal Laser Stimulation

Outline

- Introduction to Fault Attacks
  - Hardware Faults
  - Inducing Hardware Faults
  - Fault Attacks on Cryptographic Systems
  - Applying Fault Attacks to FPGAs
- Case Study: Remote PDN Fault Attacks
- Case Study: Local Thermal Laser Stimulation

Hardware Faults [1]

- Error introduced by the hardware
- Transient faults affect only a short time slice
  - e.g. caused by cosmic radiation
- Latent faults repeat after a certain period
  - e.g. Intel’s floating point division bug
- An attacker can induce transient fault by changing
  - voltage, temperature, frequency, etc.
- May change the result of a computation
  - by flipping bits in memory or registers
  - by changing the output of logic circuits
  - by creating a timing difference during computation

Inducing Hardware Faults [3]

- Device parameter variation
    - Supply voltage
        - Propagation delay is inversely related to supply voltage
        - Lowering the voltage increases delay
    - Other parameters
        - Frequency
        - Environment temperature
- Localized heating
    - Using laser with long wavelength
    - Low photon energy, no photoelectric effect
- Photoelectric effect (e.g. white light, laser)
- Induction from software (e.g. Rowhammer) [2]

Fault Attacks on Cryptographic Systems

- Differential fault analysis [4] may break
  - public key systems such as RSA [1]
  - break private key systems such as DES [4] or AES [5]
- Compute plaintext, ciphertext pairs
  - with and without inducing a fault
  - use difference in CT to recover parts of the secret

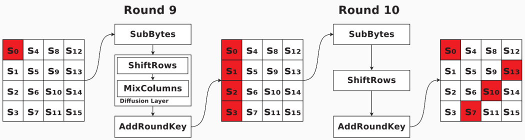


Figure 1: Fault attack on AES [6] Induce single-byte fault before round 9. Results in 4 faulty bytes in ciphertext.

Applying Fault Attacks to FPGAs

- FPGAs are commonly built in CMOS technology
- All previously mentioned strategies can be applied

- Cloud services provide FPGAs for acceleration [6]
- Remote fault attacks necessary

- Power distribution network (PDN) is shared for all FPGA blocks

Outline

Introduction to Fault Attacks

Case Study: Remote PDN Fault Attacks

- Attacker Model
- Voltage Drops in PDNs
- Disruptive Attack with Ring Oscillators
- AES Key Recovery Attack
- Countermeasures

Case Study: Local Thermal Laser Stimulation

Attacker Model [6]

- Multi-tenant architecture
  - Attacker and victim on same board
  - Separated with logical isolation
  - Shared PDN
- Attacker may reconfigure logic in assigned area
- Victim computes AES encryptions

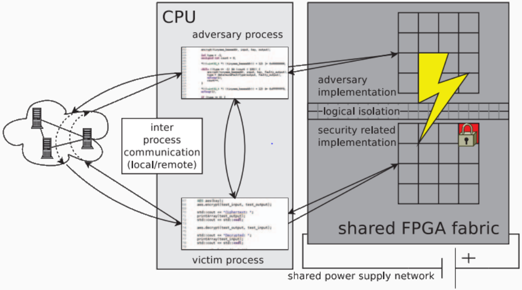

CPU
adversary process
inter process communication (local/remote)
victim process
adversary implementation
logical isolation
security related implementation
shared FPGA fabric
+
shared power supply network

Figure 2: Thread model proposed in [6]

Voltage Drops in PDNs

- A voltage drop between PDN and load is characterised by
  - IR drop
  - Inductive $L(di/dt)$ drop
- Inductive voltage drop has more impact on smaller technologies [7]
- Attacker wants a logic structure with high transient current consumption

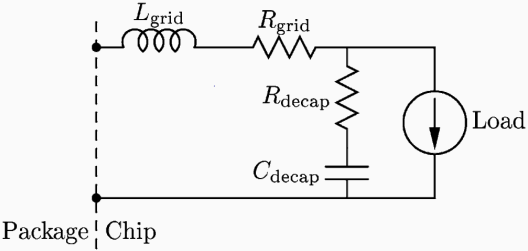


Figure 3: Simple PDN model with load [8]

Disruptive Attack with Ring Oscillators [9]

- Ring Oscillator (RO) can be built from LUTs
    - Needs about 7% to 12% of FPGA for RO structure
    - Enable RO with adjustable clock
- Sweep adjustable clock until crash occurs
- Device is inaccessible until total power reset
    - Denial of Service on cloud possible

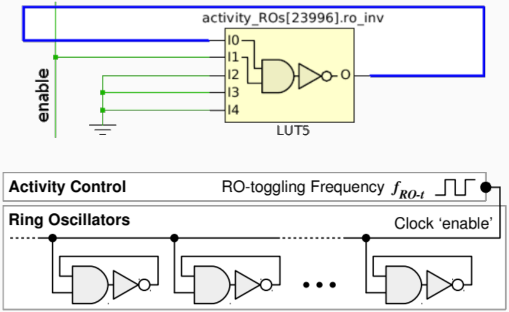


Figure 4: Ring oscillator structure proposed by [9]

AES Key Recovery Attack [6, 10]

- Attack last round of AES
  - Needs about 35% to 45% of FPGA for RO structure
  - Can also use benign designs such as AES or s1238 benchmark
  - 50% logic utilization for AES
  - 65% logic utilization for s1238
- Self-calibrating attack
  - Iterate until 1 byte in round 9 is flipped
  - Variable frequency, duty-cycle and activation delay

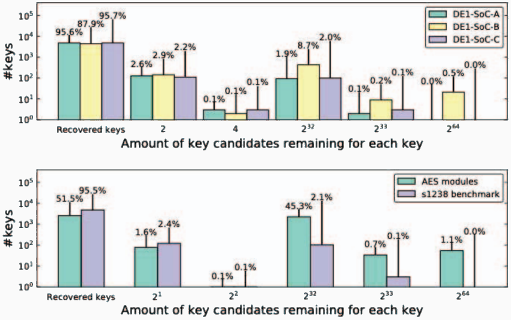


Figure 5: Results of attack proposed in [10]

Countermeasures [6]

- Adjust timing for critical logic paths
  - Increase timing margins
  - Delay elements invalidate output if close timing violation
- Separate power regions for each user
  - Decreases efficiency for multi-tenant operation
- Check bitstream for combinational loops and ROs
  - Difficult to implement
  - Polynomial complexity
  - Attacker can hide malicious logic
  - ”Benign” faulting structures (e.g. AES) are not detected

Outline

Introduction to Fault Attacks

Case Study: Remote PDN Fault Attacks

Case Study: Local Thermal Laser Stimulation

- Attacker Model
- Seebeck Voltage affecting SRAM Cells
- Bitstream Key Extraction
- Countermeasures

Attacker Model [11]

- Physical access to FPGA
  - Optional training device
- Stimulate device area with laser
  - From the backside of the chip
- Measure device parameters
  - Voltage induced by thermal heating
- Extract information from SRAM
  - Bitstream encryption key
  - Encrypted configuration data

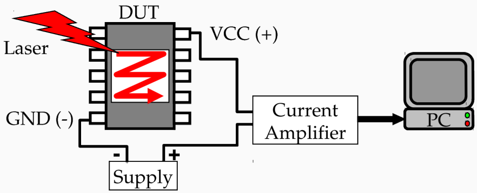


Figure 6: Monitoring device parameters during laser stimulation [11]

Seebeck Voltage Generation [12]

- Photon energy of laser smaller than silicon bandgap
  - Causes heating of drain terminal
  - Temperature gradient at metal-silicon junction
- Seebeck effect generates voltage
  - Measurable if channel exists between source and drain

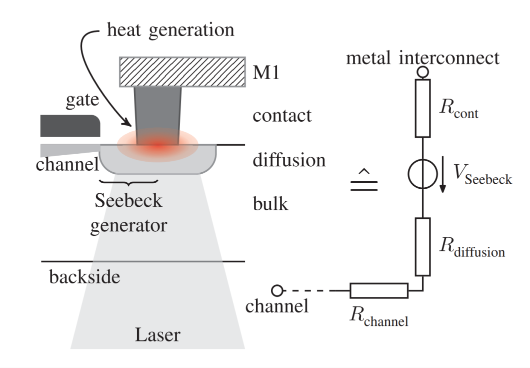


Figure 7: Seebeck voltage generation [12]

Seebeck Voltage in SRAM Cells [12]

- Seebeck voltage affects only low-ohmic transistors
  - No change in left branch
  - Gate voltage of right PMOS increases
- Sub-threshold conduction
  - Measurable current between VDD and GND
  - Extract state of SRAM cells

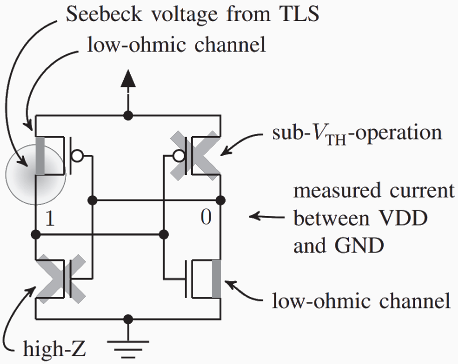
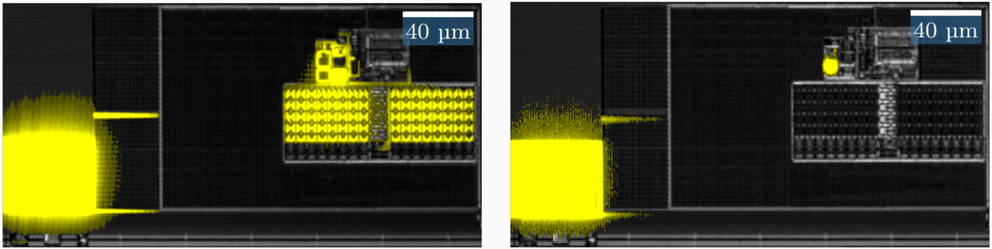


Figure 8: Seebeck voltage in SRAM cell [12]

Bitstream Key Extraction [11]

- Encryption key is stored securely
  - Battery-backed RAM or eFuses
  - No read out possible
  - BBRAM is tamper-resistant during runtime
- Attack can be mounted in power down state
  - Only the BBRAM will be active
  - Reduces additional noise
- Required steps
  - (i) BBRAM localization
  - (ii) Verify key dependency of stimulation response
  - (iii) Key bit localization
  - (iv) Key extraction

(i) BBRAM Localization [11]

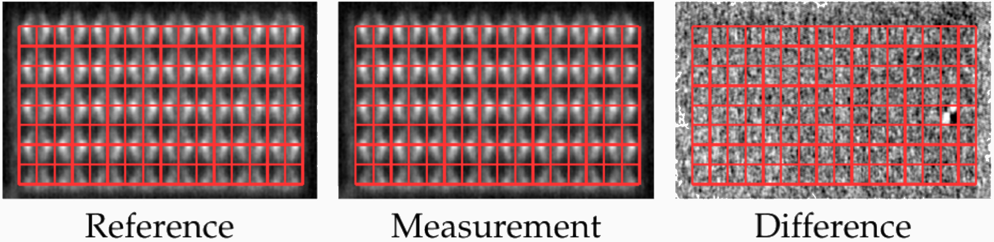


(a) BBRAM key storage active.

(b) BBRAM key storage inactive.

Figure 9: BBRAM localization [11]

(ii) Verify Key Dependency of Stimulation [11]



Reference

Measurement

Difference

Figure 10: Difference between zero key and 1 active key bit [11]

(iii) Key Bit Localization [11]

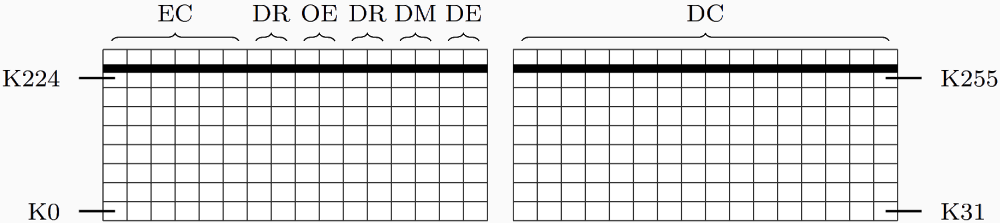
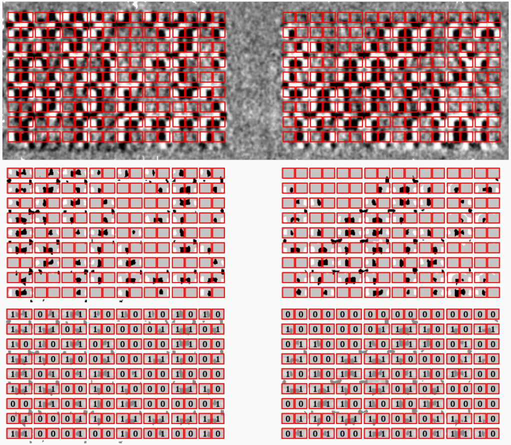


Figure 11: Key bit map after localization experiment [11]

(iv) Key Extraction [11]



```
1 1 | 0 1 | 1 1 | 1 0 | 1 0 | 1 0 | 1 0 | 1 0
1 1 | 1 1 | 0 1 | 1 0 | 0 0 | 0 1 | 1 1 | 0 1
1 0 | 1 0 | 1 1 | 0 1 | 0 0 | 0 0 | 1 1 | 0 0
1 1 | 1 0 | 1 0 | 0 1 | 0 0 | 1 1 | 1 0 | 0 1
1 1 | 0 1 | 0 1 | 1 1 | 0 1 | 0 0 | 1 0 | 0 0
1 1 | 1 1 | 0 0 | 1 0 | 1 0 | 0 0 | 1 1 | 1 0
0 0 | 1 1 | 0 1 | 1 0 | 1 1 | 0 0 | 0 0 | 0 1
0 1 | 0 0 | 0 1 | 1 0 | 1 1 | 1 1 | 1 1 | 1 1
1 1 | 0 0 | 0 1 | 0 0 | 1 0 | 0 1 | 0 0 | 1 0
```

```
0 0 | 0 0 | 0 0 | 0 0 | 0 0 | 0 0 | 0 0 | 0 0
1 0 | 0 0 | 0 0 | 0 1 | 1 1 | 1 0 | 1 0 | 1 1
0 1 | 1 0 | 0 0 | 1 0 | 1 1 | 1 0 | 0 1 | 0 0
1 1 | 0 0 | 1 1 | 1 1 | 1 0 | 0 0 | 0 1 | 1 0
1 0 | 1 0 | 1 1 | 1 1 | 0 1 | 1 0 | 1 1 | 0 0
1 1 | 1 1 | 1 0 | 1 1 | 0 1 | 0 1 | 0 0 | 0 0
0 0 | 1 1 | 1 0 | 1 0 | 1 0 | 1 1 | 0 0 | 0 0
0 1 | 1 0 | 1 1 | 1 0 | 0 1 | 0 1 | 1 1 | 1 0
0 1 | 0 1 | 0 0 | 1 1 | 0 1 | 0 1 | 1 1 | 1 0
```

Figure 12: Key extraction with decoded key [11]

Countermeasures [11]

- Key obfuscation
  - Use red key, store black key
  - Stored key is encrypted with metalized key
  - Store metalized key in eFuses
  - Prevents reverse-engineering
  - Cloning to another device still possible
  - Prevent cloning by including unique device ID
- Sensing the laser
  - Impossible with light sensors
  - Possible with battery-powered temperature sensors
- Introduce noise source
  - Hides data-dependent current

References i

[1] D. Boneh, R. A. DeMillo, and R. J. Lipton, **On the importance of checking cryptographic protocols for faults,** in International conference on the theory and applications of cryptographic techniques, Springer, 1997, pp. 37–51.

[2] D. Gruss, C. Maurice, and S. Mangard, **Rowhammer. js: A remote software-induced fault attack in javascript,** in Detection of Intrusions and Malware, and Vulnerability Assessment: 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings 13, Springer, 2016, pp. 300–321.

[3] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, **The sorcerer's apprentice guide to fault attacks,** Proceedings of the IEEE, vol. 94, no. 2, pp. 370–382, 2006.

References ii

[4] E. Biham and A. Shamir, **Differential fault analysis of secret key cryptosystems,** in Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17, Springer, 1997, pp. 513–525.

[5] C. Giraud, **Dfa on aes,** in Advanced Encryption Standard–AES: 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers 4, Springer, 2005, pp. 27–41.

[6] J. Krautter, D. R. 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, pp. 44–68, 2018.

[7] K. Arabi, R. Saleh, and X. Meng, **Power supply noise in socs: Metrics, management, and measurement,** IEEE Design & Test of Computers, vol. 24, no. 3, pp. 236–244, 2007.

References iii

[8] A. V. Mezhiba and E. G. Friedman, **Scaling trends of on-chip power distribution noise,** in Proceedings of the 2002 international workshop on System-level interconnect prediction, 2002, pp. 47–53.

[9] D. R. Gnad, F. Oboril, and M. B. Tahoori, **Voltage drop-based fault attacks on fpgas using valid bitstreams,** in 2017 27th International Conference on Field Programmable Logic and Applications (FPL), IEEE, 2017, pp. 1–7.

[10] J. Krautter, D. R. E. Gnad, and M. B. Tahoori, **Remote and stealthy fault attacks on virtualized fpgas,** in Design, Automation & Test in Europe Conference & Exhibition, DATE 2021, Grenoble, France, February 1-5, 2021, IEEE, 2021, pp. 1632–1637.

[11] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, **Key extraction using thermal laser stimulation: A case study on xilinx ultrascale fpgas,** IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 573–595, 2018.

References iv

[12] C. Boit, C. Helfmeier, D. Nedospasov, and A. Fox, **Ultra high precision circuit diagnosis through seebeck generation and charge monitoring,** in Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), IEEE, 2013, pp. 17–21.