SCIENCE
PASSION
TECHNOLOGY

Remote Power Attacks on FPGAs

Béla Lemle

Digital System Integration and Programming (2023 WS)

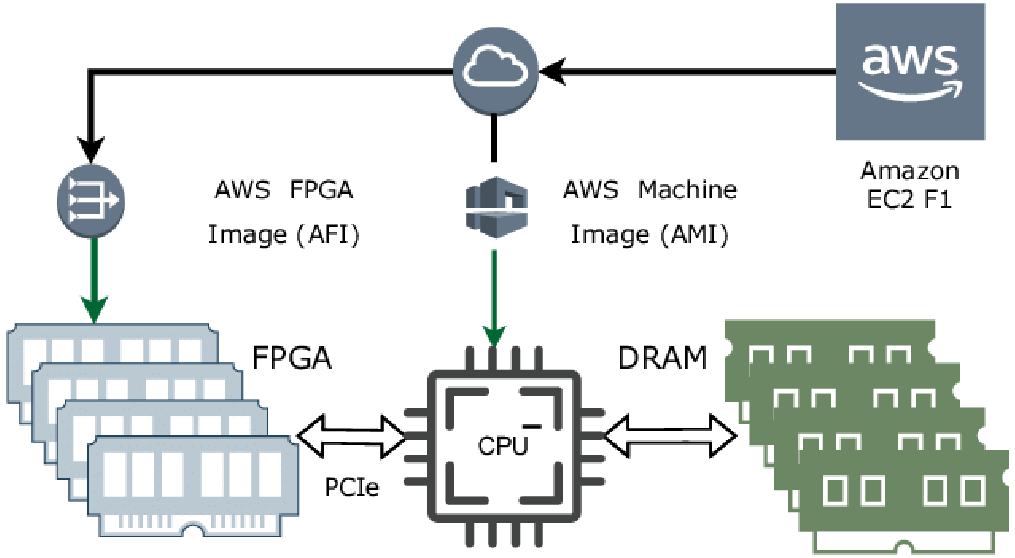
27. November 2023

Agenda

- Power Analysis Attacks
- Remote Power Analysis Attacks
- Implementation of On-Chip Sensors
- Remote Attacks with On-Chip Sensors + Countermeasures
- Software Monitor-Based Remote Attacks

Motivation

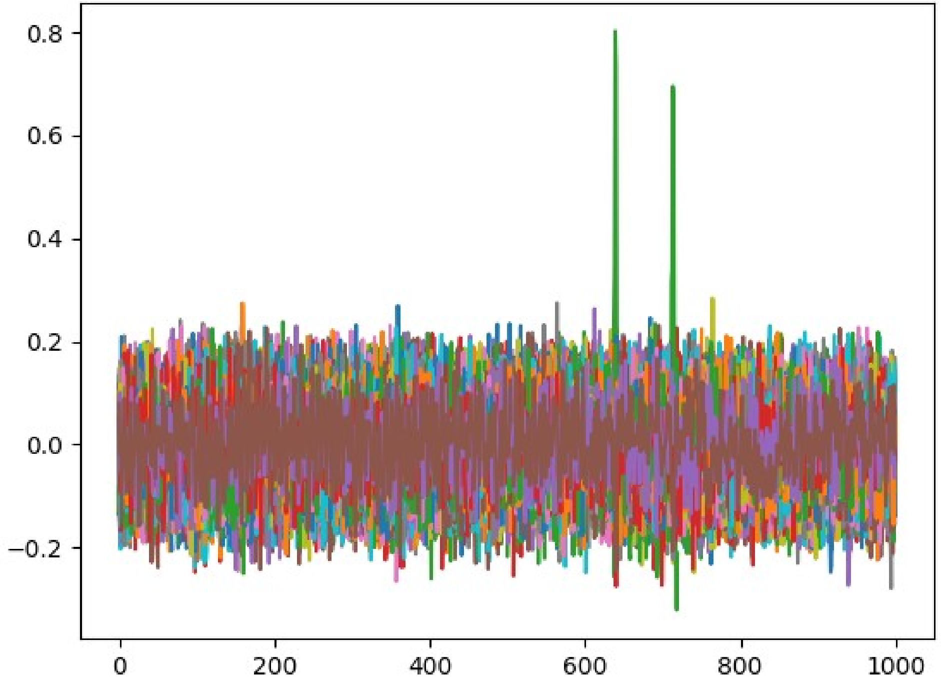
- Cloud FPGAs
- Multiple users use the FPGA simultaneously
- Opens the door for a new class of attacks
- Logic-level isolation is applied
- Same PDN -> attacker may instantiate a sensor to monitor voltage fluctuations



Amazon AWS EC2 F1 instance architecture [KAMMSB22]

Power Analysis Attacks

- Differential Power Analysis (**DPA**) [KJJ99]
  - Measure the power consumption of a device with different input values
  - Predict power consumption by using a power model (e.g Hamming Weight)
  - Scan through the traces looking for the highest correlation
- Correlation Power Analysis (**CPA**) -> a variation of **DPA** [BCO04]
- Limitations
  - Attacker needs **physical access**
  - **Special tools** needed (e.g. oscilloscope)
- Algorithmic-level mitigations
  - **Hiding**
  - **Masking**



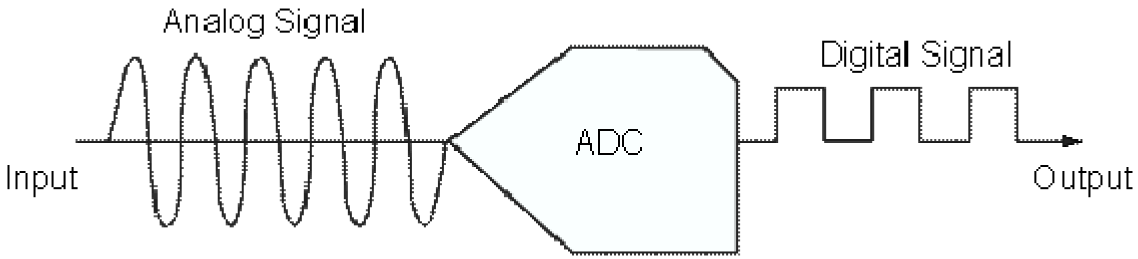
DPA Correlation traces on AES

Remote Power Analysis

- Side-Channel Attack (**SCA**)
  - Byproduct of transistor level physics [MRDLB21]
- Differences to **Power Analysis**
  - No **equipment** or **physical access** needed
  - Root cause is in the hardware design -> redesign needed
  - No proximity required -> mount over e.g **Ethernet**
- Not a …
  - Far-field EM attack
  - Software-induced fault attack (e.g RowHammer)
  - Software-based microarchitectural attack (e.g Spectre)

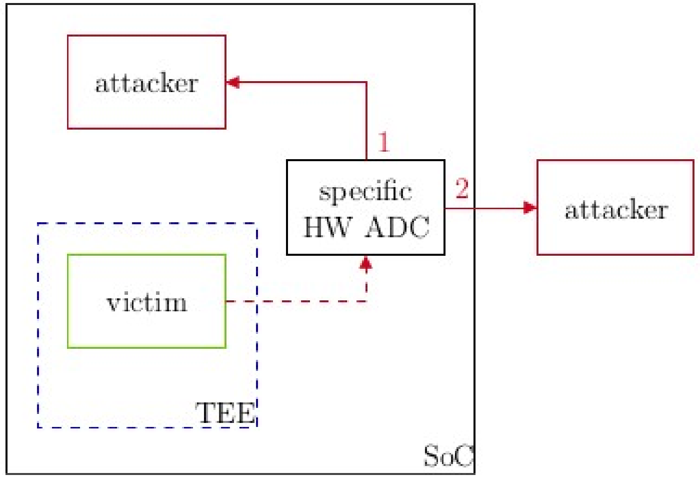
Attacks using Analog-to-Digital converter

- Analog-to-Digital Converter (ADC) converts analog signals to digital signals
- Digital logic (executing cryptographic operations) triggers noise in e.g. ADC [MRDLB21]



Analog to Digital conversion

Attack 1 using ADC [MRDLB21]

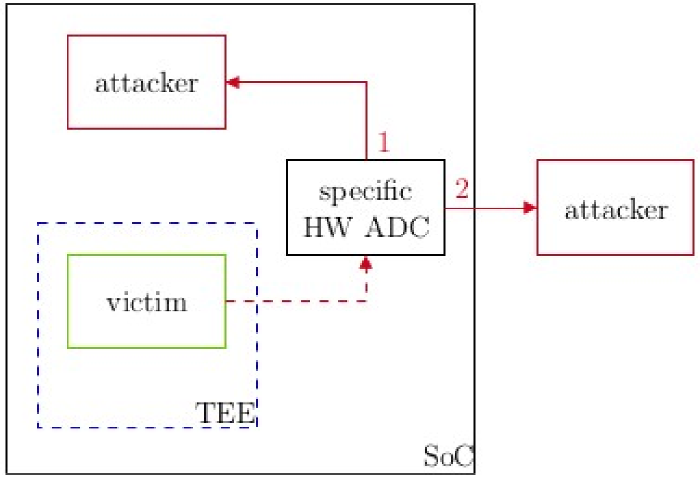


Attack Model [MRDLB21]

- Full or partial access to the ADC
- Read during cryptographic operation (different task)
- Both AES-128 and RSA (mbedTLS) show leakage [GKT19]
- Works even without the ADC being connected to supply voltage
- With Correlation Power Analysis the leakage can be used to learn sensitive information

Attack 2 using ADC [MRDLB21]

- The cryptographic algorithm is executed in TEE (Trusted Execution Environment)
- SAML11 hardware AES accelerator → hardware-level isolation [OD19]
- Assumption: attacker can start the execution from the insecure side
- Retrieve all AES-128 key bytes
  - Correlation Power Analysis
  - S-Box of the last round
  - Hamming Weight Model



Attack Model[MRDLB21]

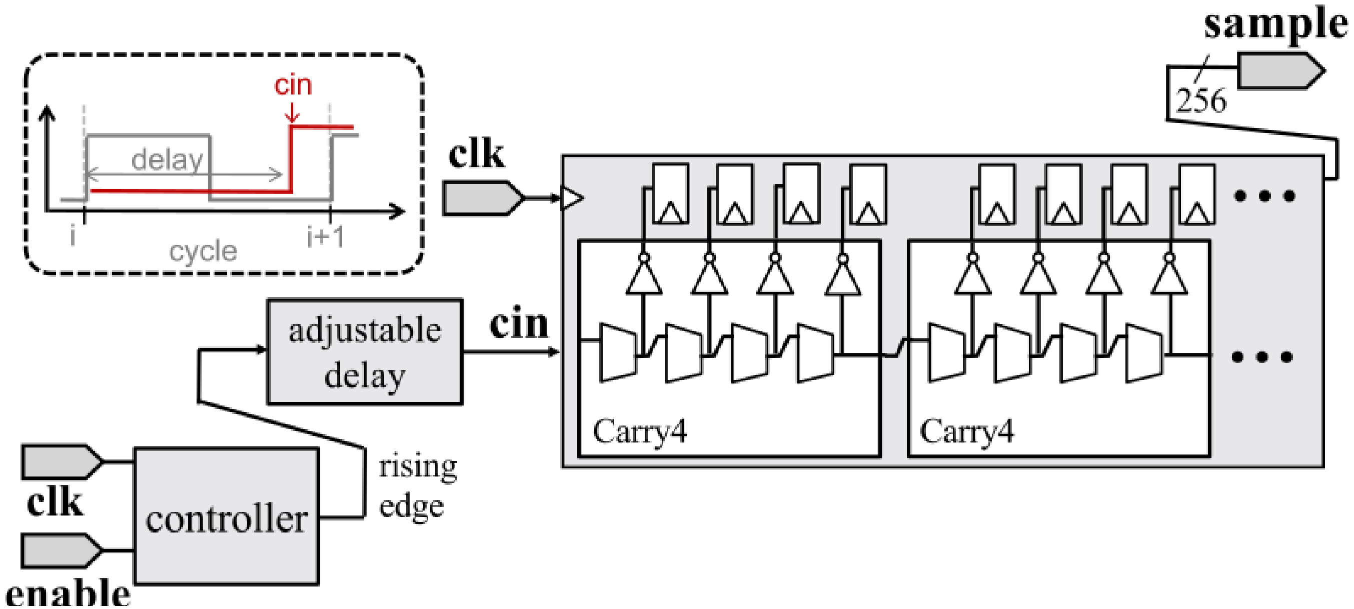
Countermeasures [OD19]

- No measurement during security critical operations
- Move ADC and other peripherals to the secure world (TEE)
- Validate peripherals before encryption/decryption
    - Not valid -> suspend encryption/decryption
    - Valid continue with the operation
- Protocol-level solution
    - Limit the max usage number of a key

On-Chip Voltage Sensors

- Sensors implemented on the programmable logic
- Monitor the fluctuations on the Power Distribution Network (PDN) [GDTLM19]
  - Even with total hardware logic isolation
- Time-to-Digital Converter (TDC)[GDTLM19]
  - Convert propagation delay variations into digital representation [SGMT18]
- Ring Oscillator (RO)[GDTLM19]
  - Measures the propagation delay through the RO

TDC-based Voltage Sensor Implementation

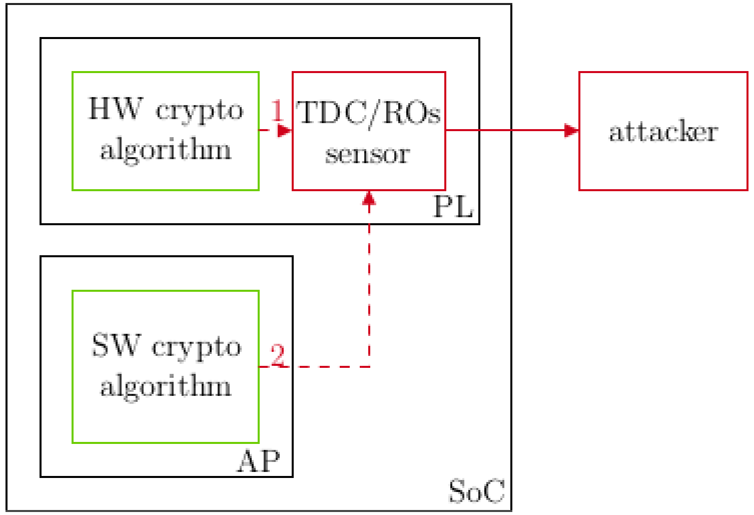


Schematic view of TDC Sensor implementation[MDL+22]

- Adjustable delay line (calibration)
- Carry4 or Carry8 primitives (provided by Xilinx)
- Rising edge of the system clock stores to flip-flops
- Output “sample” is the hamming weight of the flip-flops

TDC-based Remote Attack 1 (Gravellier et al) [GDTLM19]

- Cloud FPGA rental -> insert untrusted IP, reconfigure bitstream
- Target software and hardware implementation of AES
- Sensor is part of the Programmable Logic
- Sensor is inserted on the same die as the Application Processor
- Mount CPA attack -> get the AES key
  - hardware implementation 1000 traces
  - software implementation (tinyAES, OpenSSL) 100 000 traces

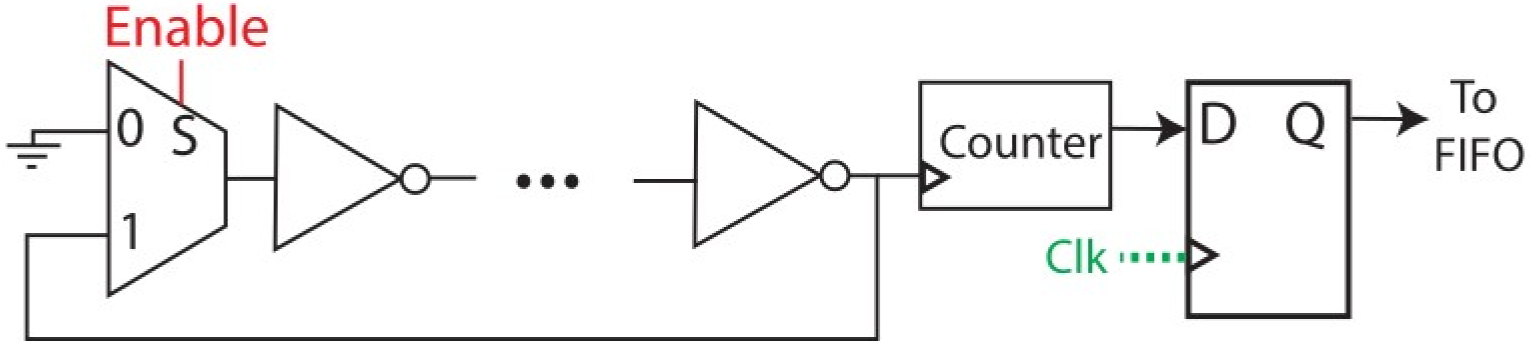


Attack Model[MRDLB21]

Countermeasure [MRDLB21]

- Independent power supply for each FPGA chip in the cloud -> cost
- Classical countermeasures
  - Masking, Hiding
  - Hardens the key recovery
- Restrict/limit access to delay-line registers
- Remove delay-lines -> not feasible

RO-based Voltage Sensor Implementation



Schematic view of RO Sensor implementation[MDL+22]

- Similar to TDC, measures propagation delay
- Store number of oscillations of the previous clock cycle

RO-based Remote Attack 1 (Gravellier er al.) [GDTLM19]

- RO-based sensor is used to measure the voltage variations
- 128-bit register value refreshed after AES rounds creates a usable supply voltage fluctuations
- Targeting the last round of an AES crypto module with CPA
- With 16 ROs 78 000 traces needed to recover AES key
- With 64 ROs 8000 traces needed to recover the key

RO-based Remote Attack 2 (Zhao and Shuh) [ZS18]

- Attack FPGA used by multiple users
- Targeting the Square & Multiply of an RSA cryptomodule
    - Exponent = 1 -> high switching activity in LUTs and FFs
    - Exponent = 0 -> low switching activity, only multiplier
- Get the correct keys with just a visual inspection

Countermeasure [ZS18]

- Use active fences to protect cryptographic modules
  - Randomly activated (PRNG)
  - Activate the needed amount based on module’s voltage fluctuation
- Increase the noise on the SoC
  - Lower SNR
  - Reduce resolution of the voltage fluctuations
- Decreases leakage also if using ADCs
- Classical mitigations are always possible (masking, hiding)
- Filter designs by analyzing netlist -> not easy as ROs are valid

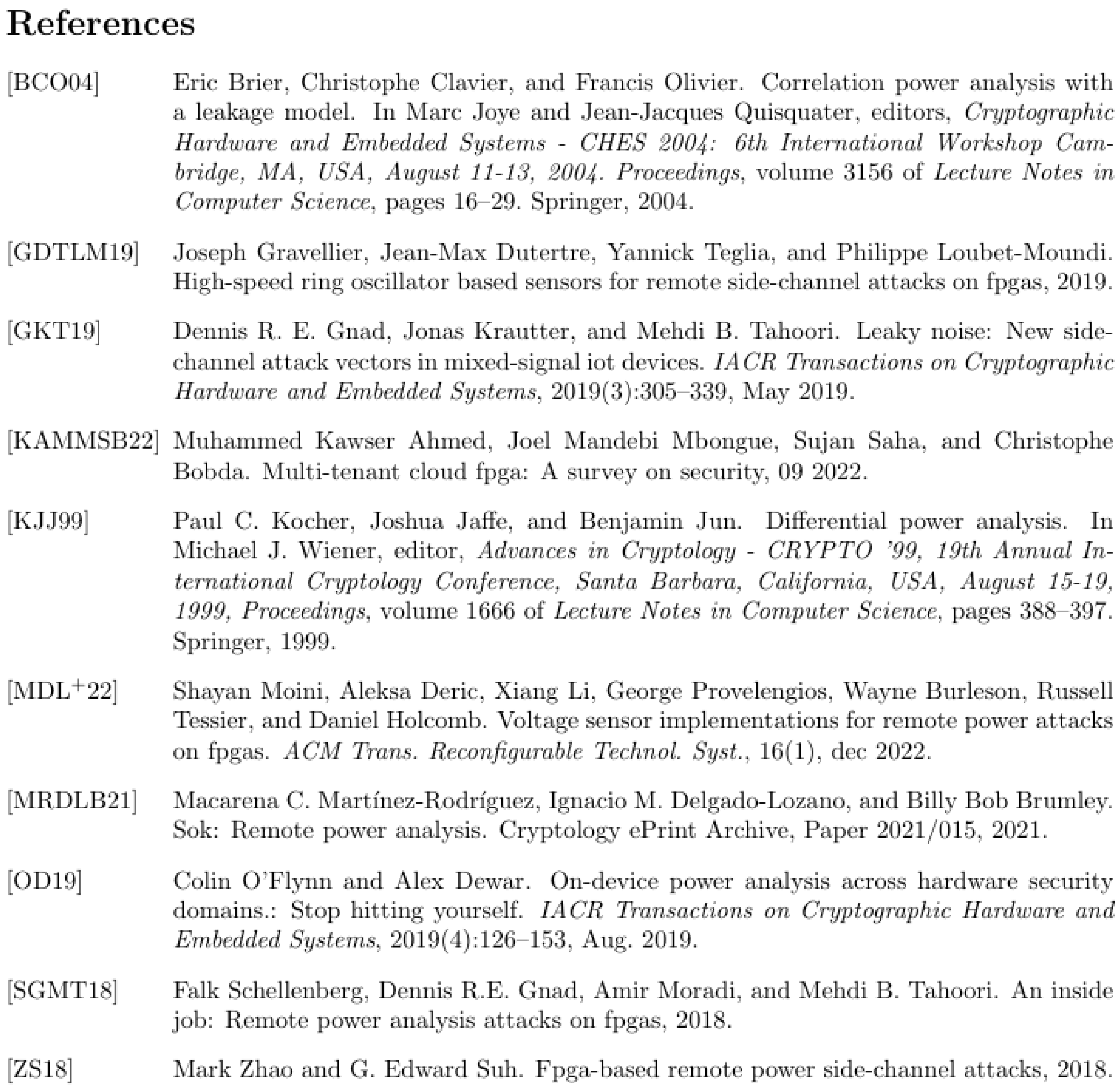
Software Monitor-based Remote Attacks [MRDLB21]

- Vendor applications to measure voltage fluctuations
- Intel Running Average Power Limit (**RAPL**)
    - Application/interface
    - Control core frequency
    - Control core voltage
    - Monitor power consumption
    - High resolution
- CPU implementation on FPGA in cloud **possible? vulnerable?**

Conclusion

- Remote Power Attacks pose a serious threat
- No additional equipment or physical access needed
- On-Chip Voltage Sensors can be implemented without restriction
- Attacks are possible and no real countermeasure yet
- More vulnerable components and more sophisticated techniques

Thank you for your attention!



References

[BCO04] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.

[GDTLM19] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, and Philippe Loubet-Moundi. High-speed ring oscillator based sensors for remote side-channel attacks on fpgas, 2019.

[GKT19] Dennis R. E. Gnad, Jonas Krautter, and Mehdi B. Tahoori. Leaky noise: New side-channel attack vectors in mixed-signal iot devices. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(3):305–339, May 2019.

[KAMMSB22] Muhammed Kawser Ahmed, Joel Mandebi Mbongue, Sujan Saha, and Christophe Bobda. Multi-tenant cloud fpga: A survey on security, 09 2022.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[MDL$^+$22] Shayan Moini, Aleksa Deric, Xiang Li, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb. Voltage sensor implementations for remote power attacks on fpgas. *ACM Trans. Reconfigurable Technol. Syst.*, 16(1), dec 2022.

[MRDLB21] Macarena C. Martínez-Rodríguez, Ignacio M. Delgado-Lozano, and Billy Bob Brumley. Sok: Remote power analysis. Cryptology ePrint Archive, Paper 2021/015, 2021.

[OD19] Colin O'Flynn and Alex Dewar. On-device power analysis across hardware security domains.: Stop hitting yourself. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(4):126–153, Aug. 2019.

[SGMT18] Falk Schellenberg, Dennis R.E. Gnad, Amir Moradi, and Mehdi B. Tahoori. An inside job: Remote power analysis attacks on fpgas, 2018.

[ZS18] Mark Zhao and G. Edward Suh. Fpga-based remote power side-channel attacks, 2018.