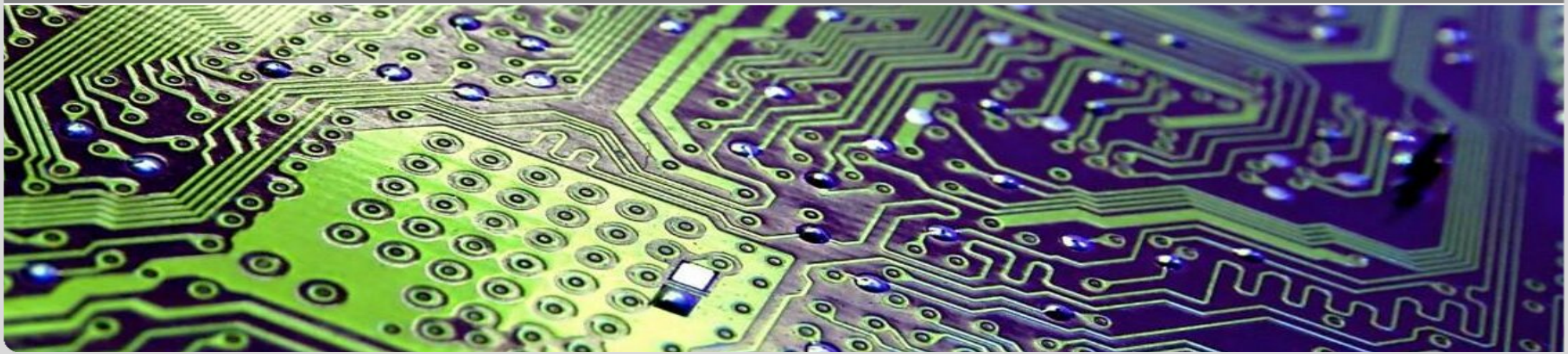
Karlsruhe Institute of Technology

Secure sharing of FPGAs in the Cloud: New Challenges at the Technology Level

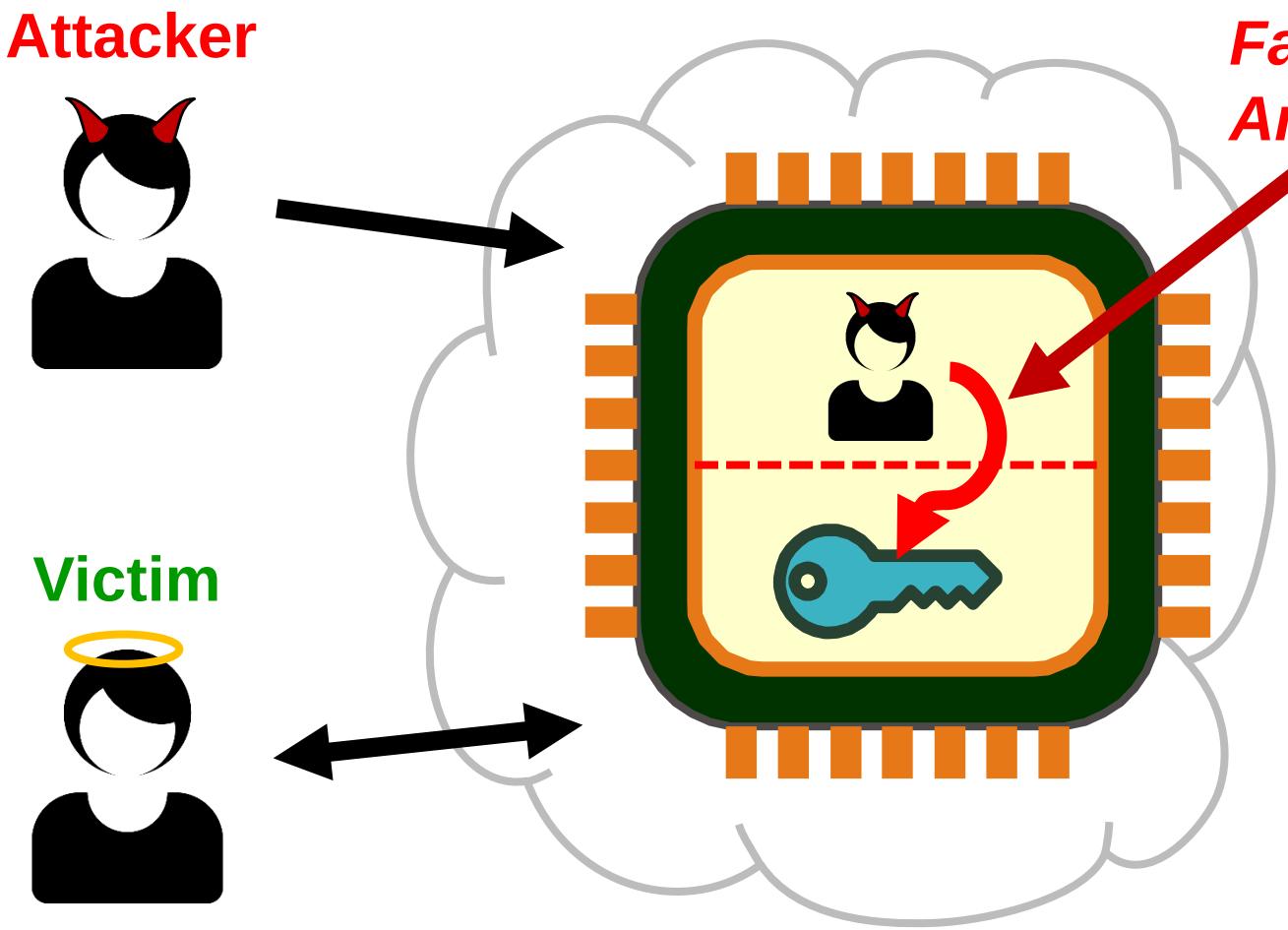
Experimentation Part

Dennis Gnad, Jonas Krautter, Mehdi Tahoori

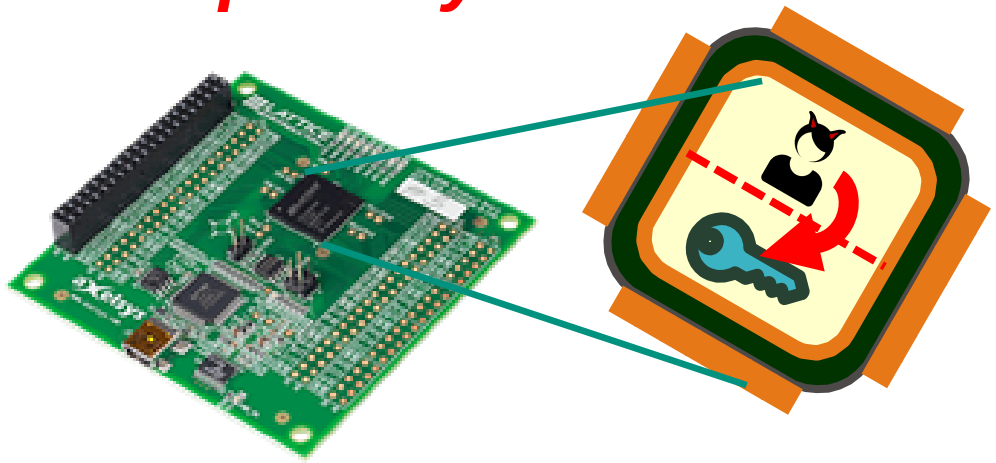
INSTITUT FÜR TECHNISCHE INFORMATIK – CHAIR OF DEPENDABLE NANO COMPUTING



Physical Fault and Side-Channel Attacks

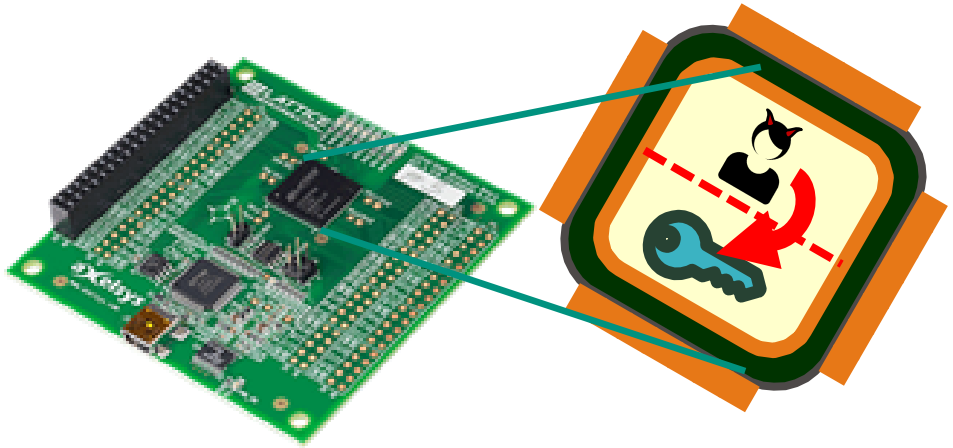


Setup that you will use:



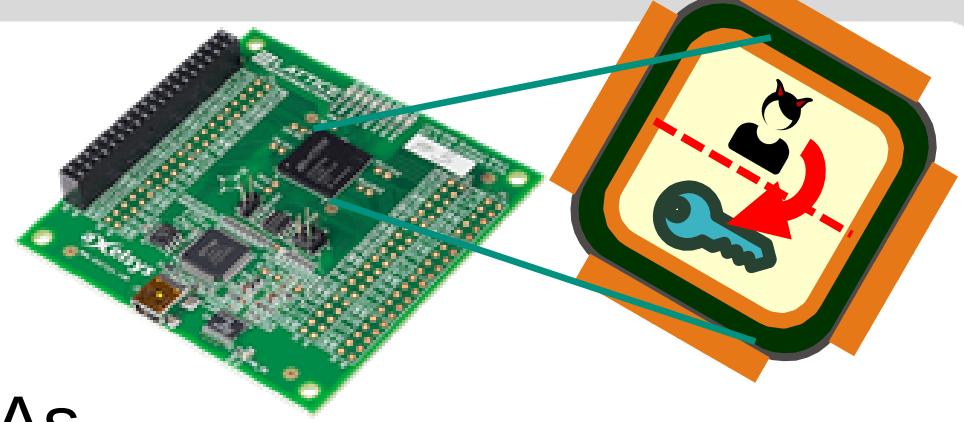
[Images: pixabay.com, wikimedia.org]

Agenda of the Practical Part



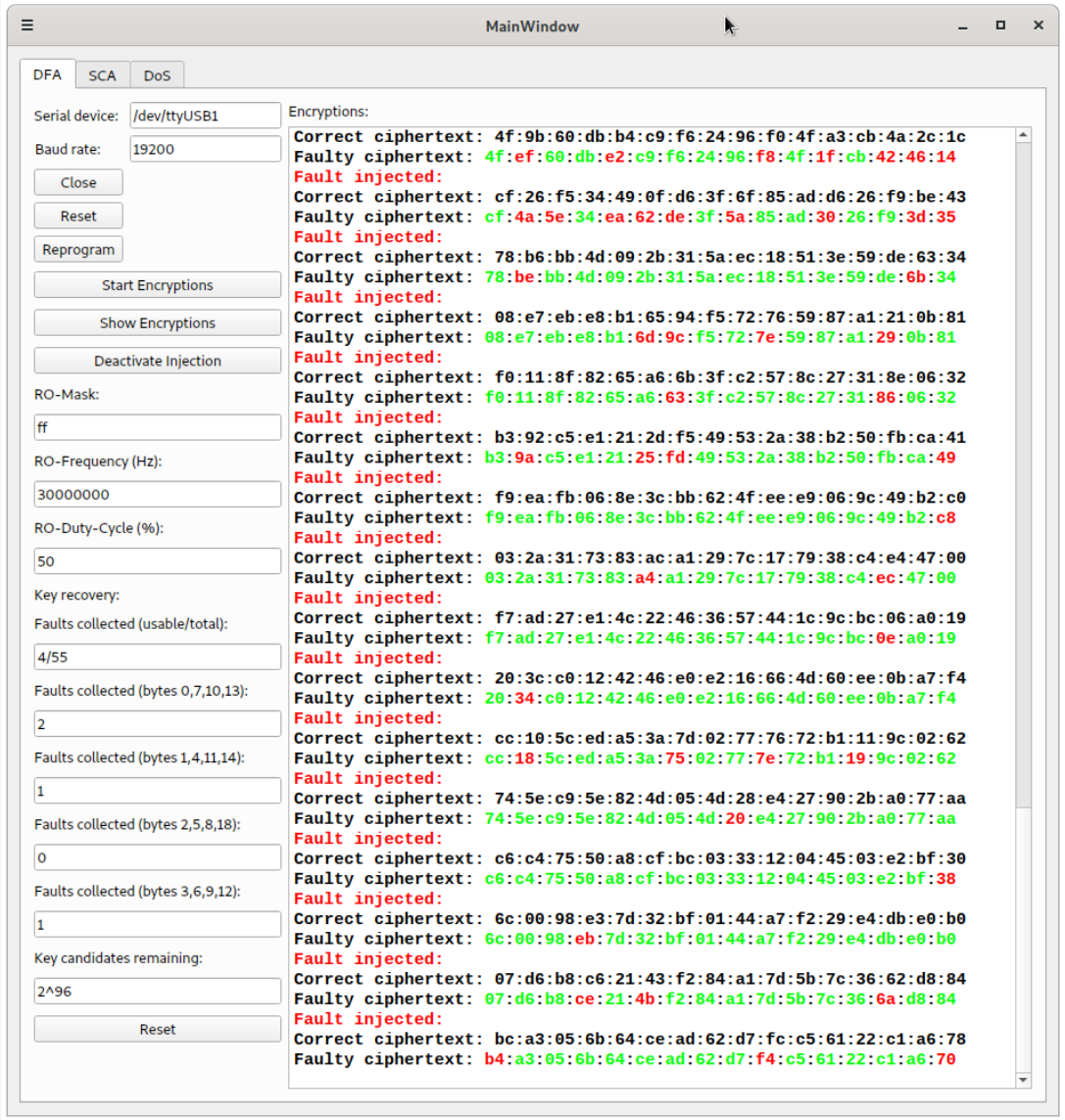
- Introduction
- Background
  - FPGAs, AES
- Side-Channel Attacks
  - Background and Presentation on Xilinx PCIe Board
- Fault Attacks
  - Background and Presentation on Intel PCIe Board
- Hands-on Part (You!)
  - CPA + DFA + DoS on Lattice FPGA Demo Boards

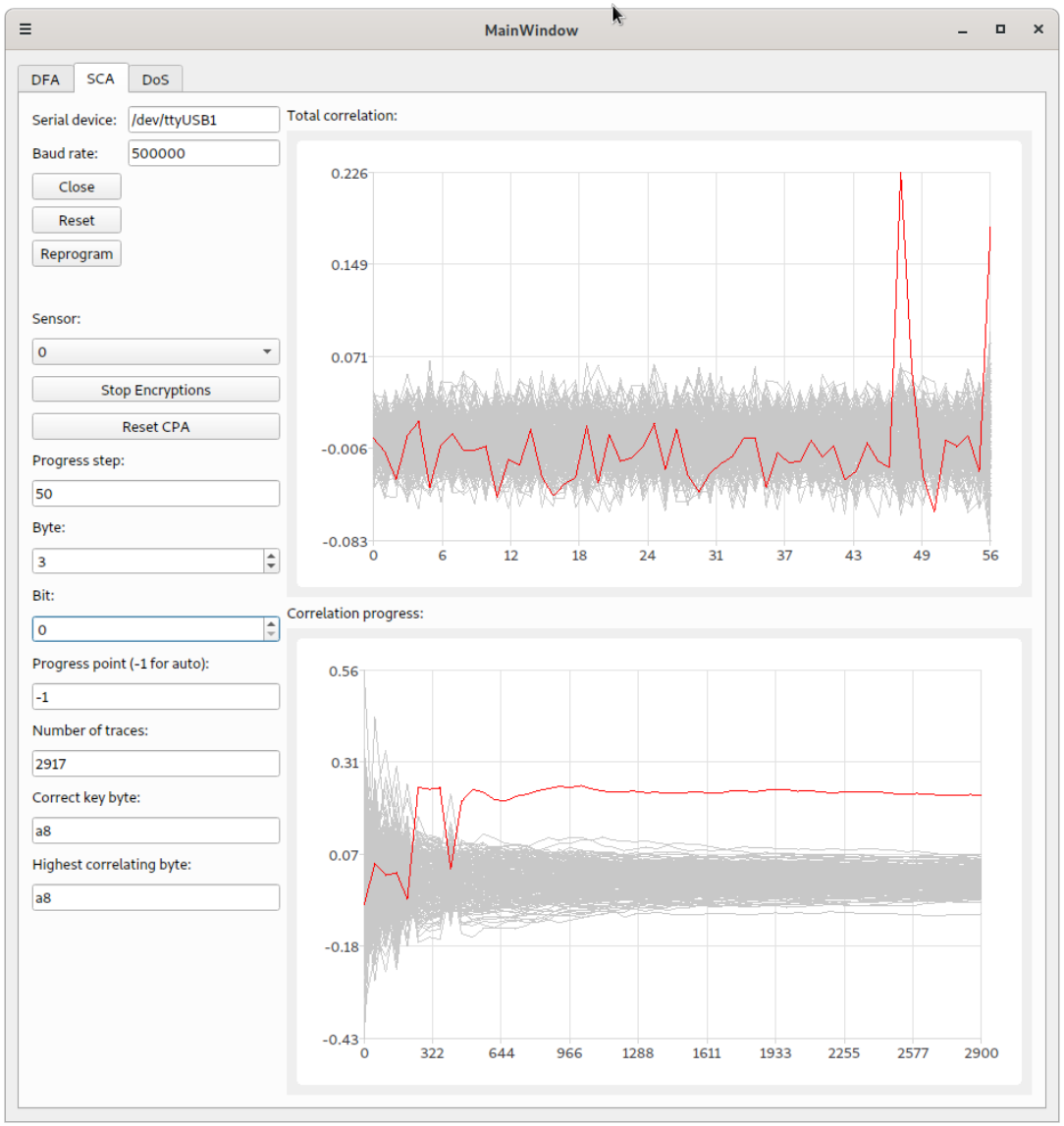
Introduction – What will you do here?

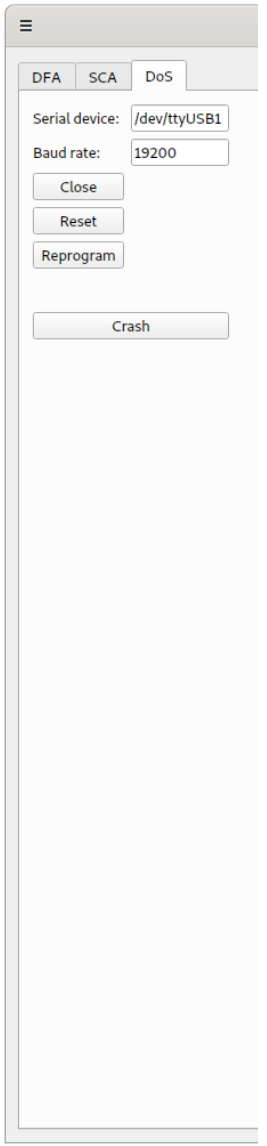


- All types of electrical-level attacks in FPGAs
  - Differential Fault Analysis (DFA)
  - Correlation Power Analysis (CPA)
  - Crash / Denial-of-Service based on Faults (DoS)
  - (Category of non-invasive attacks)
- No direct FPGA coding (but source code is available)
  - https://git.informatik.kit.edu/i83/security/nessy21

Introduction – GUI

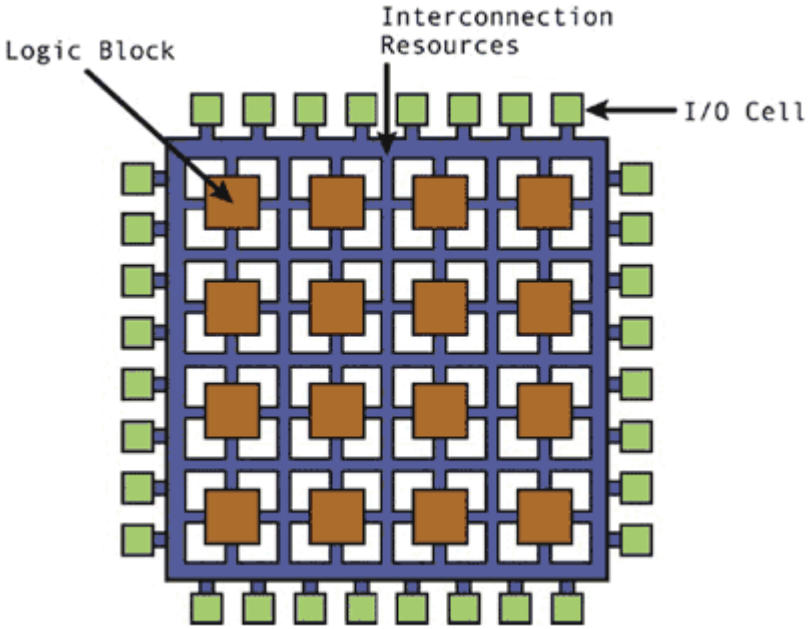


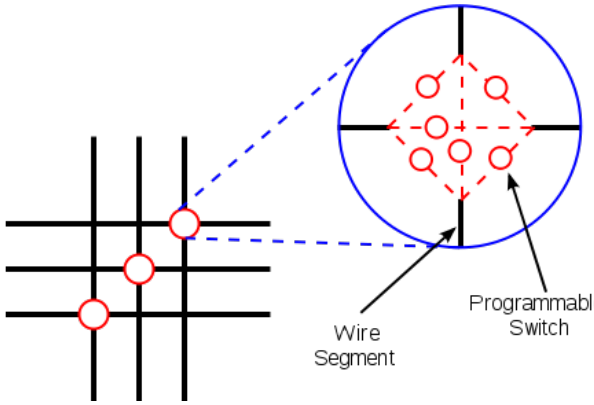


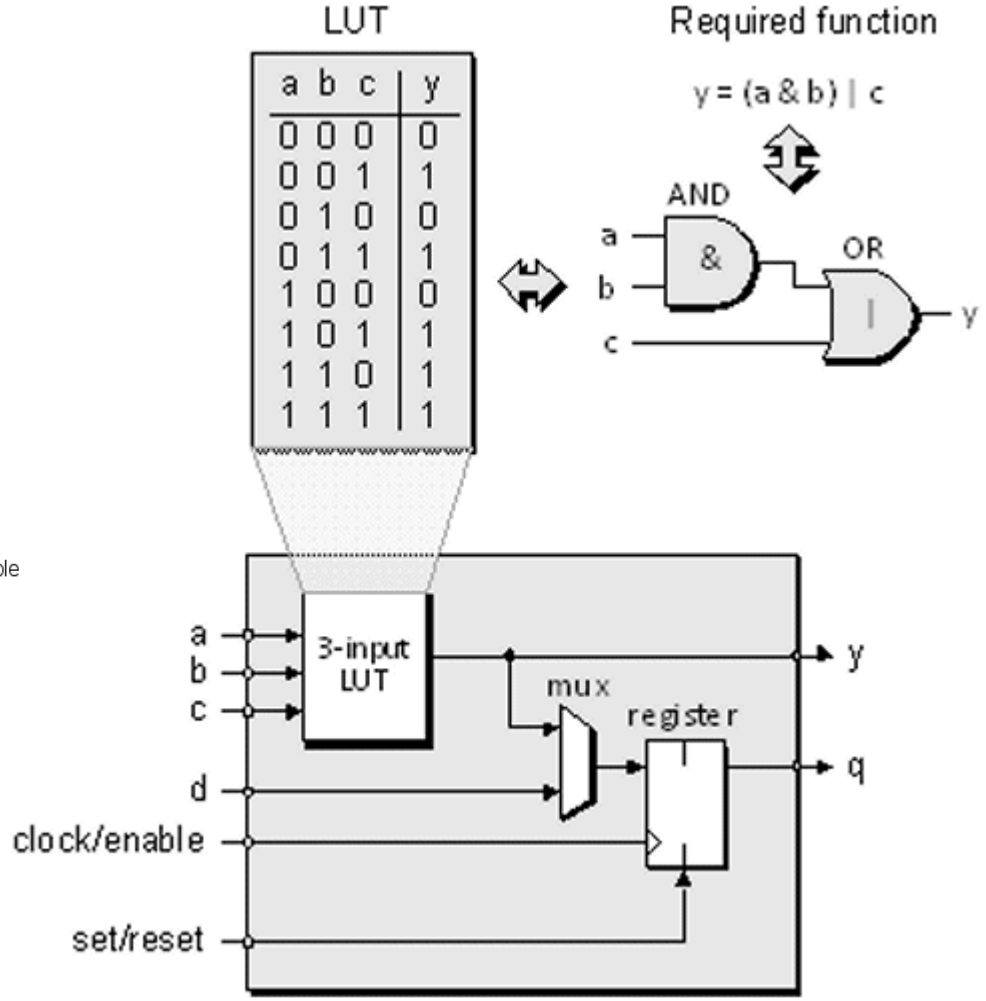


Background – FPGAs

- “Programmable Hardware”





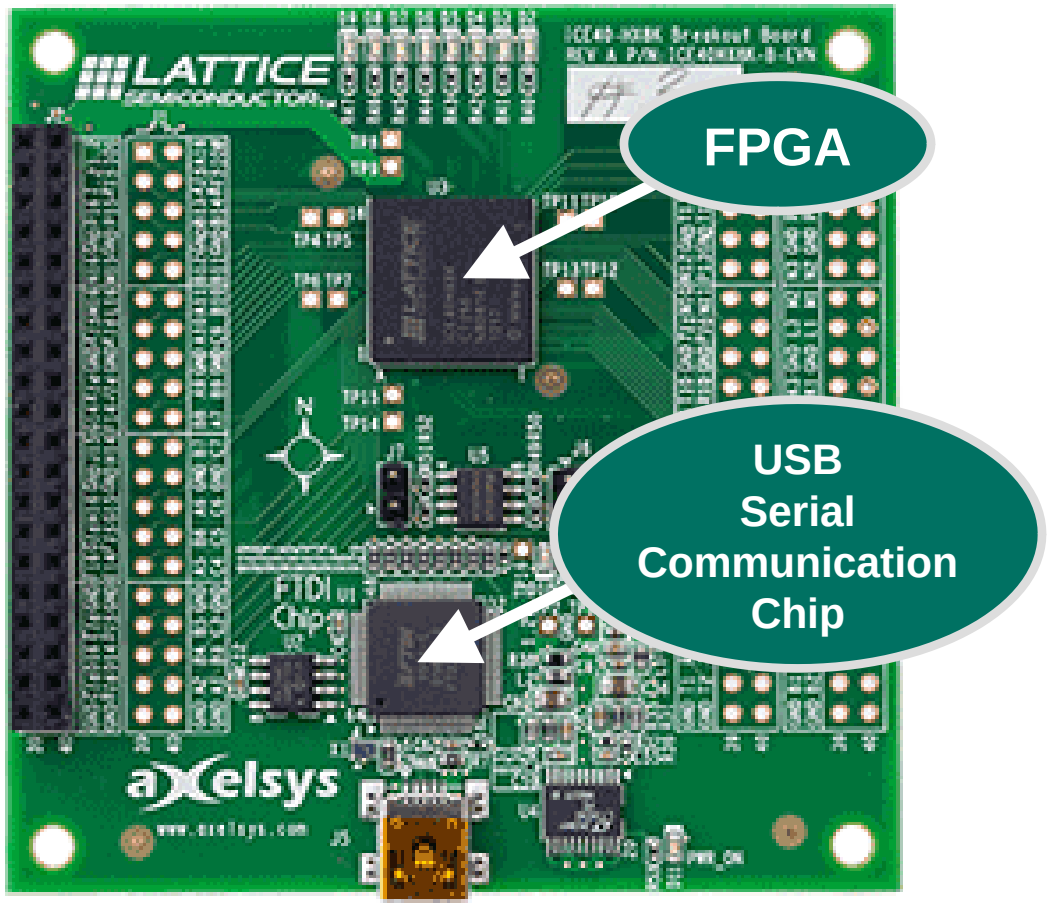


- Accelerating algorithms in hardware
- Prototyping & glue logic & many more

[src: Wikipedia]

Board that you will use

- Lattice HX8K Breakout Board
- Tiny compared to PCIe Accelerators!
  - 8k vs. 1M programmable logic elements
- Yet, very similar in technology

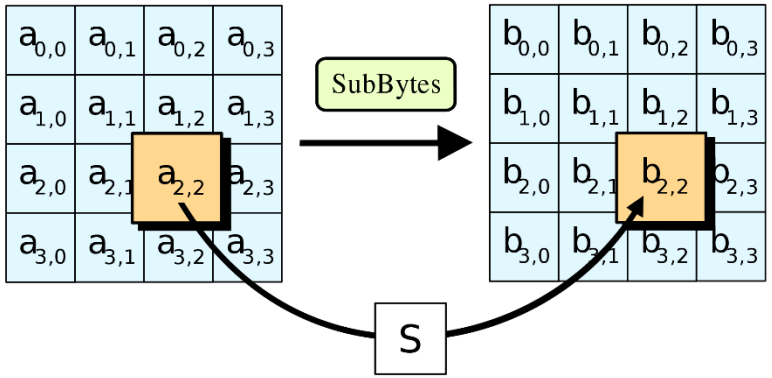


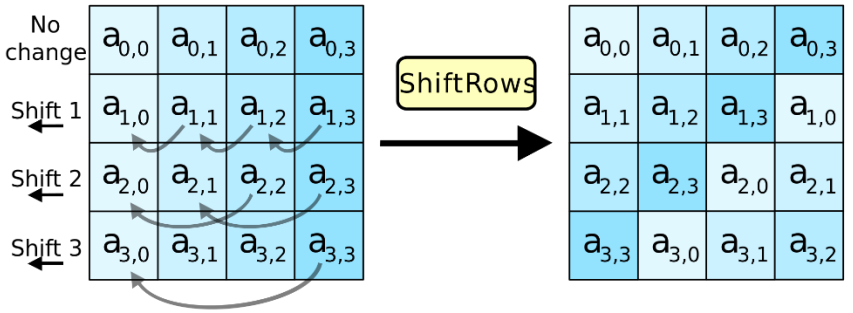
Background – Advanced Encryption Standard (AES) 1/2

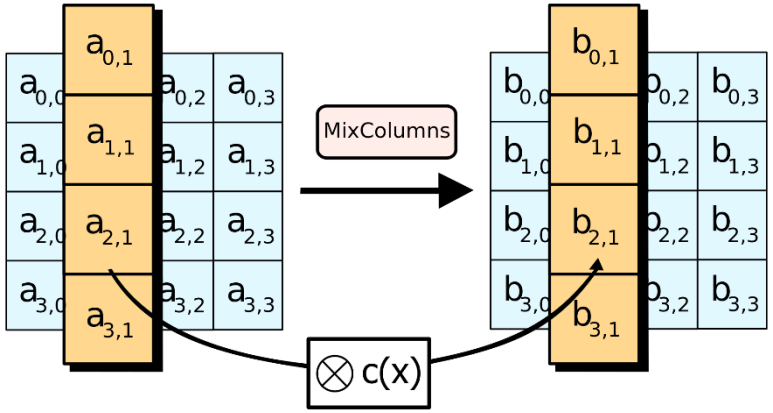
- Victim of our DFA and CPA attacks
- Symmetric Block Cipher with 128/192/256-bit
- Round-based operation in 10/12/14 rounds, 4 basic operations:
  - SubBytes – Substitution (non-linear)
  - ShiftRows – Permutation/Transposition
  - MixColumns – Permutation/Diffusion (not in the last round)
  - AddRoundKey – XOR Round Subkey (computed from 128/192/256-bit key)
- For more: The NIST Standard Document is very helpful!

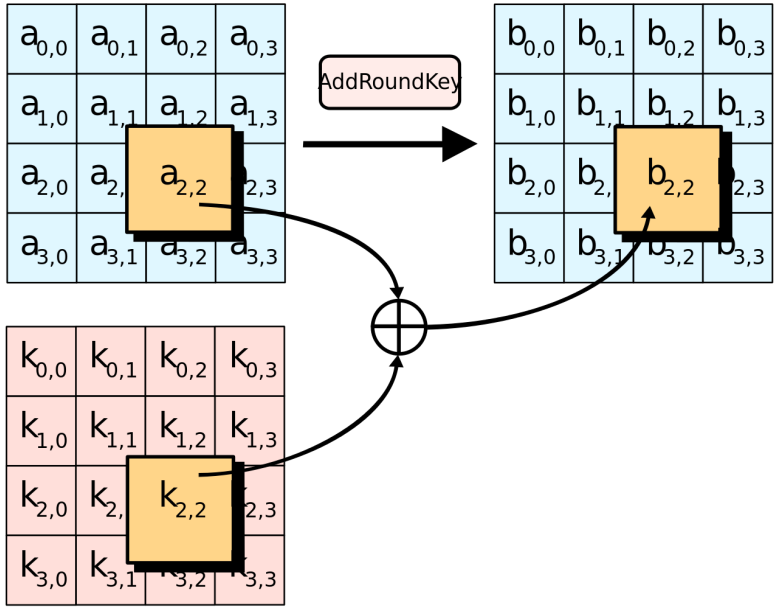
Background – Advanced Encryption Standard (AES) 2/2

- Operations on “State Matrix”









[src: Wikipedia]

Our AES Implementation

- 4x Parallel SubBytes Operations, 4 Clock Cycles
  = 4 SBoxes, implemented in logic
- ShiftRows on the entire Matrix, 1 Clock Cycle
- MixColumns, 1 Clock Cycle
- AddRoundKey, 1 Clock Cycle
- Executed after each other, some transition cycles between

Power Analysis Side-Channel Attack with Correlation Power Analysis (CPA)

- Demonstrated on Xilinx Kintex KC705 PCIe Board
- You: Experimentation on Lattice HX8K Breakout Board

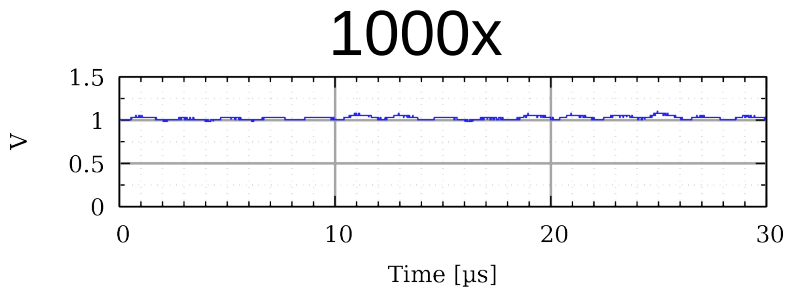
Side-Channel Attacks with Correlation Power Analysis

- The attack we will perform here: Correlation Power Analysis (CPA)
- We measure power/voltage/current but just call it “Power” here

Approach – acquire sets and correlate them:

- **Set of Measured** power values (“traces”)
  - same key, different plaintext messages
- **Multiple Sets of Modeled** power values
  - based on: guessed secret key byte and ciphertext messages

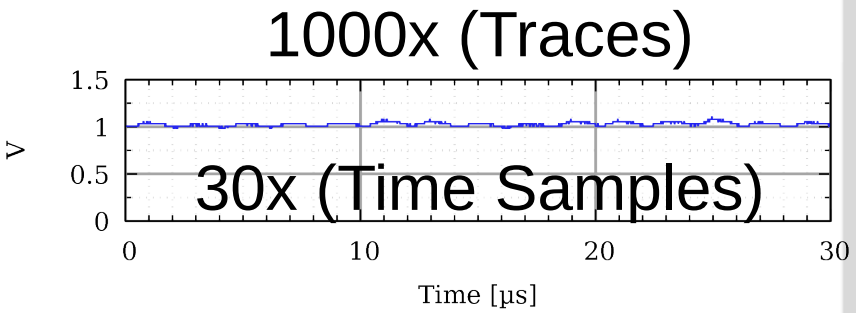
➢ Correlate measured set with each hypothesized set



256x 1000x $\mathbf{P_{modeled}(k_{hyp},c)}$

Side-Channel Attacks with Correlation Power Analysis

- Correlations separately done per time sample
- **Set of Measured** power values (“traces”)
  - same key, different plaintext messages
- **Multiple Sets of Modeled** power values
  - based on: guessed secret key byte and ciphertext message
  - dependent on operations of the algorithm:



256x (k_{hyp})

1000x (Ciphertexts)

$\mathbf{P_{modeled}(k_{hyp},c)}$

$$P_{modeled}(k_{hyp},c) = Sbox^{-1}(k_{hyp} \oplus c_i) \wedge (2^{bitpos})$$

k_{hyp} – Hypothesized/Guessed secret key byte, i.e. 0…255

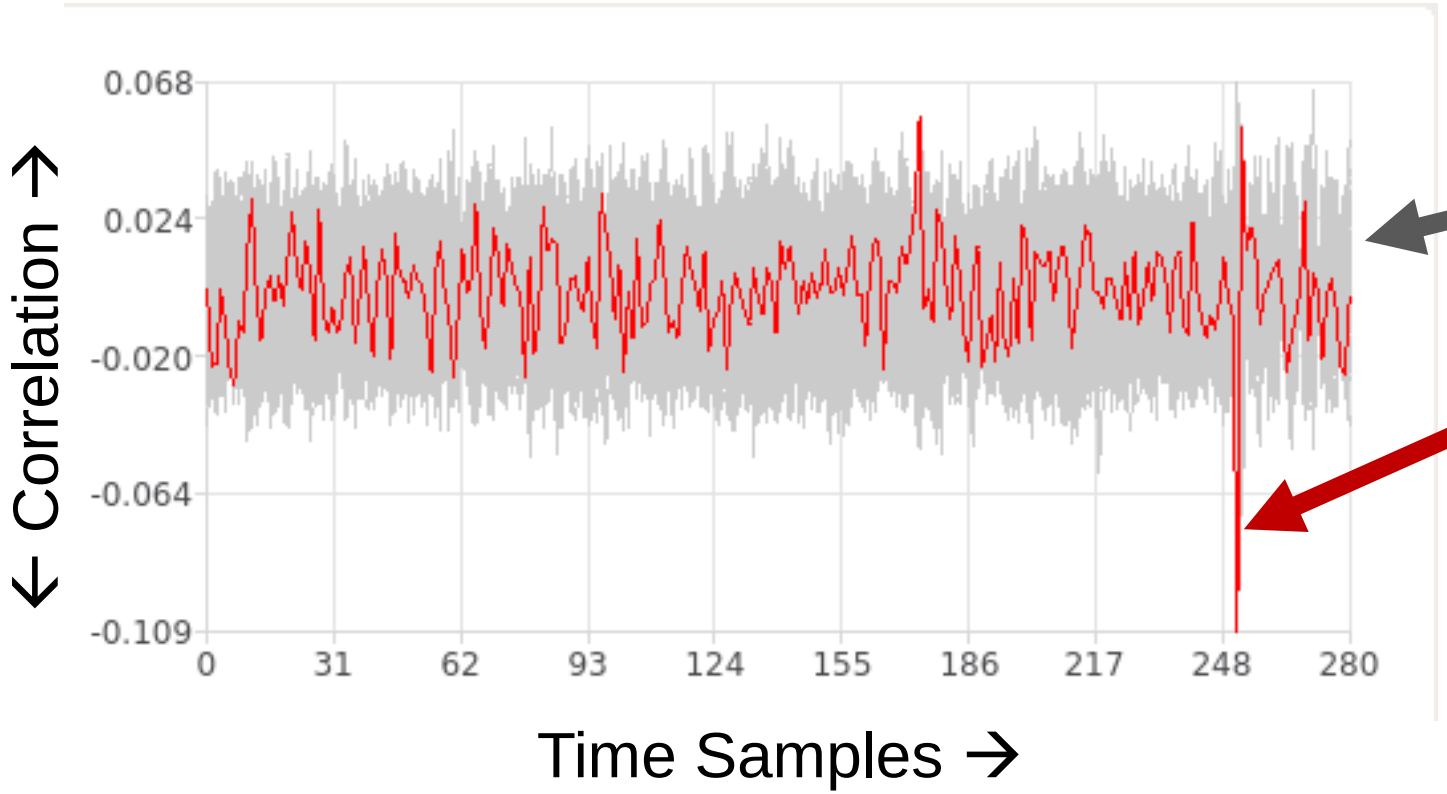
c_i – Ciphertext Byte

Detailed Approach

- Acquire Ciphertext + Power Traces over whole AES execution time
- ➢ We have multiple measured power values per plaintext (over time) “horizontally”
- ➢ We have multiple key hypothesis per plaintext/ciphertext “vertically”
- Correlate all points in time with all hypothesized key-powers
  - For instance, resulting in 256 correlation plots x time samples
  - Leakage occurs at specific time points of the operation we attack
- (If we know the exact time, only “vertical” correlation needed)

Detailed Approach

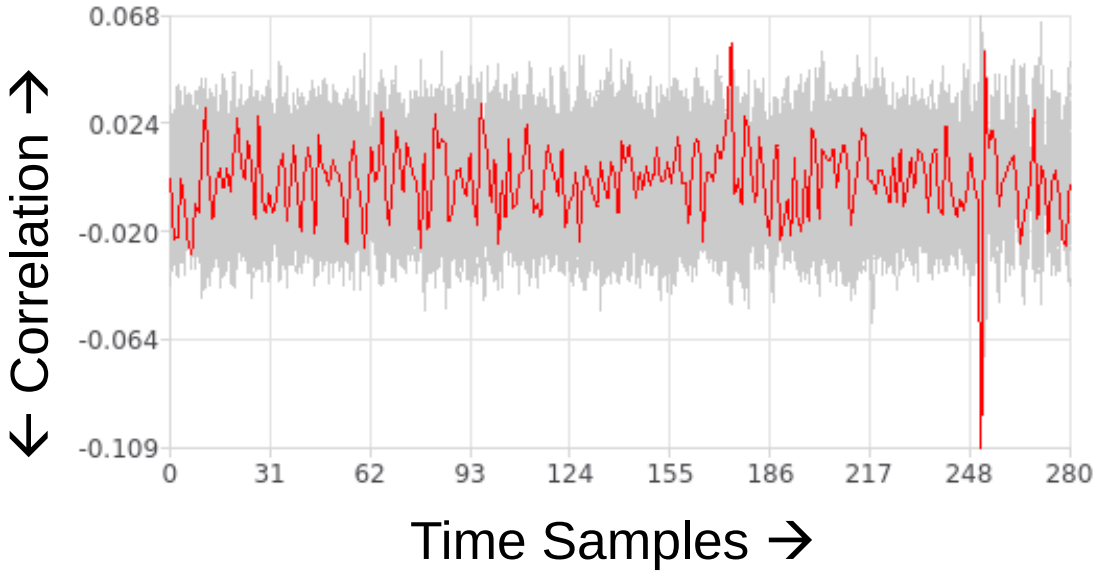
- For instance, resulting in 256 correlation plots x time samples
- Leakage occurs at specific time points of the operation we attack



256 correlation plots (correct one is red)

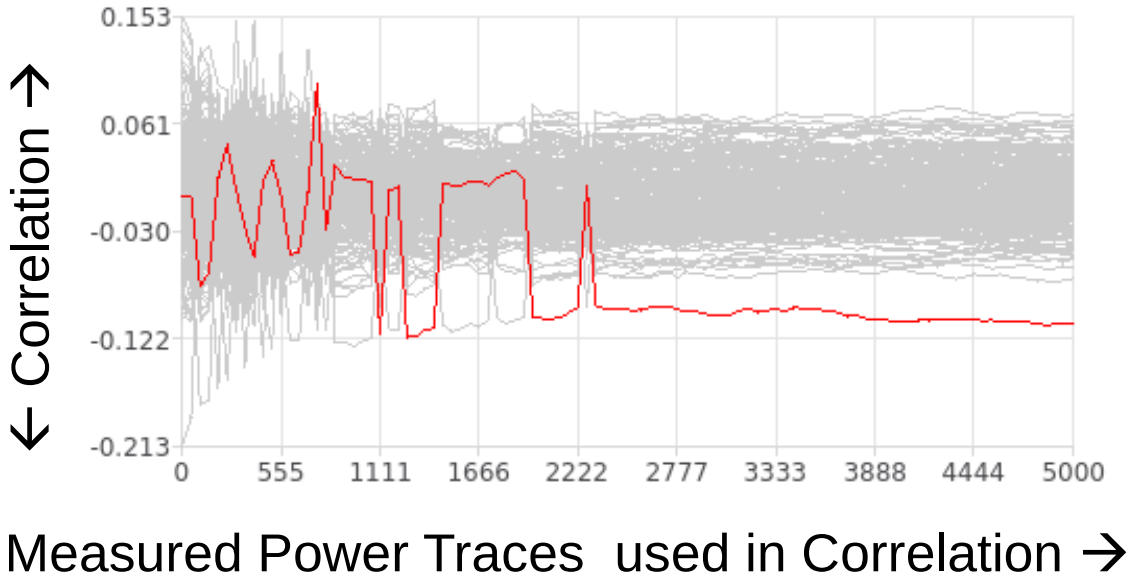
Leakage occurs at this point in time

Detailed Approach



← This is the result of correlating 5000 power traces

Plotting the most correlating time sample, depending on the amount of traces used ↓



- ***Note!*** *Most publications use only a single point in time for the progress, based on all power traces' result*
- *Obviously not possible here when plotting interim results*

Side-Channel Attacks with Correlation Power Analysis

- **Some information on the used leakage model:**

$$P_{modeled}(k_{hyp}) = Sbox^{-1}(k_{hyp} \oplus c_i) \wedge \mathbf{(2^{bitpos})}$$

k_{hyp} – Hypothesized/Guessed secret key byte, i.e. 0…255

c_i – Ciphertext Byte

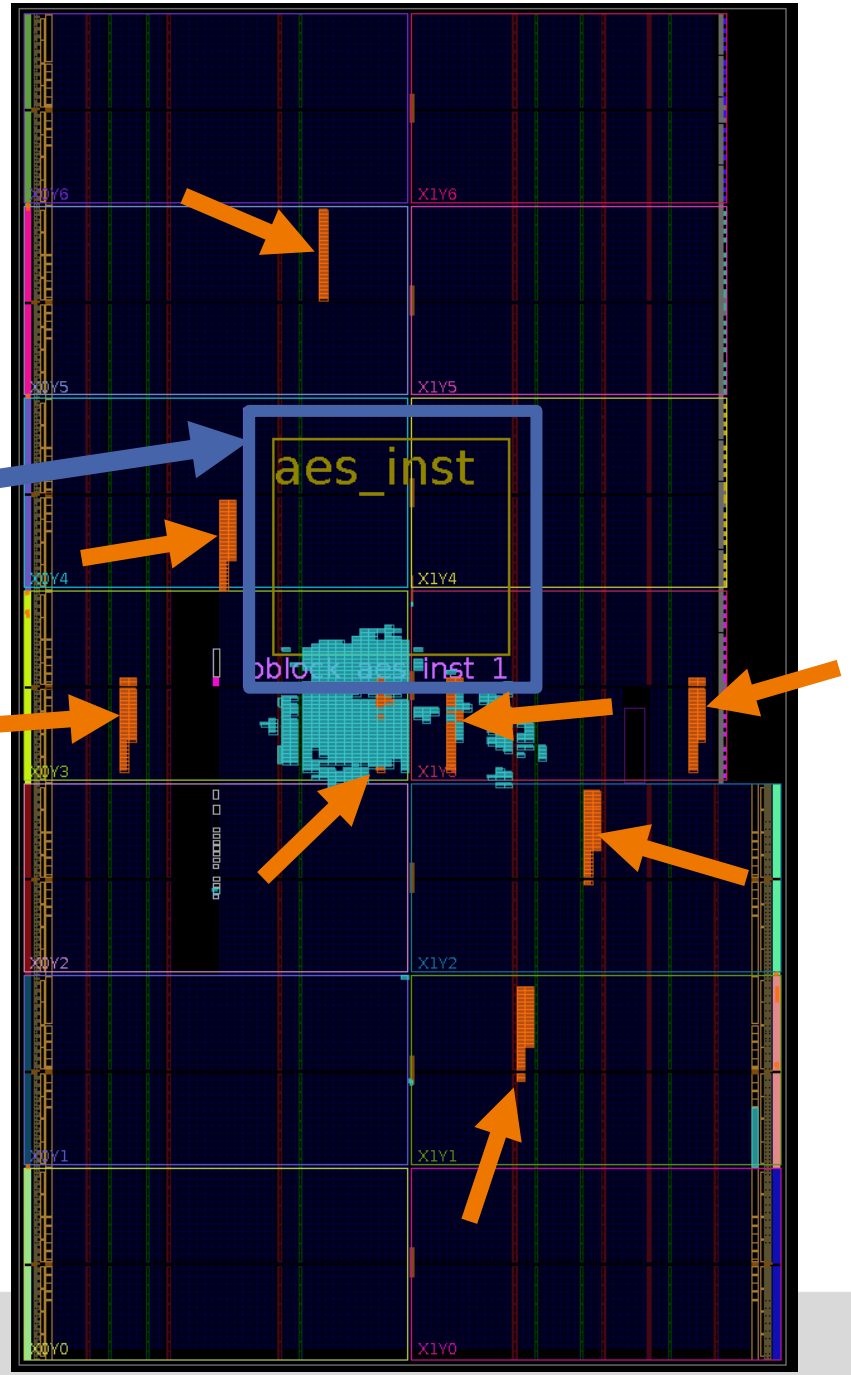
- You see $\mathbf{2^{bitpos}}$ which means we correlate single bits
- However, **one bit's leakage shows the respective byte leaks**
- Correlating only a bit can be faster than the whole byte

Live Demo

- Xilinx Kintex KC705 PCIe Board

Kintex KC705

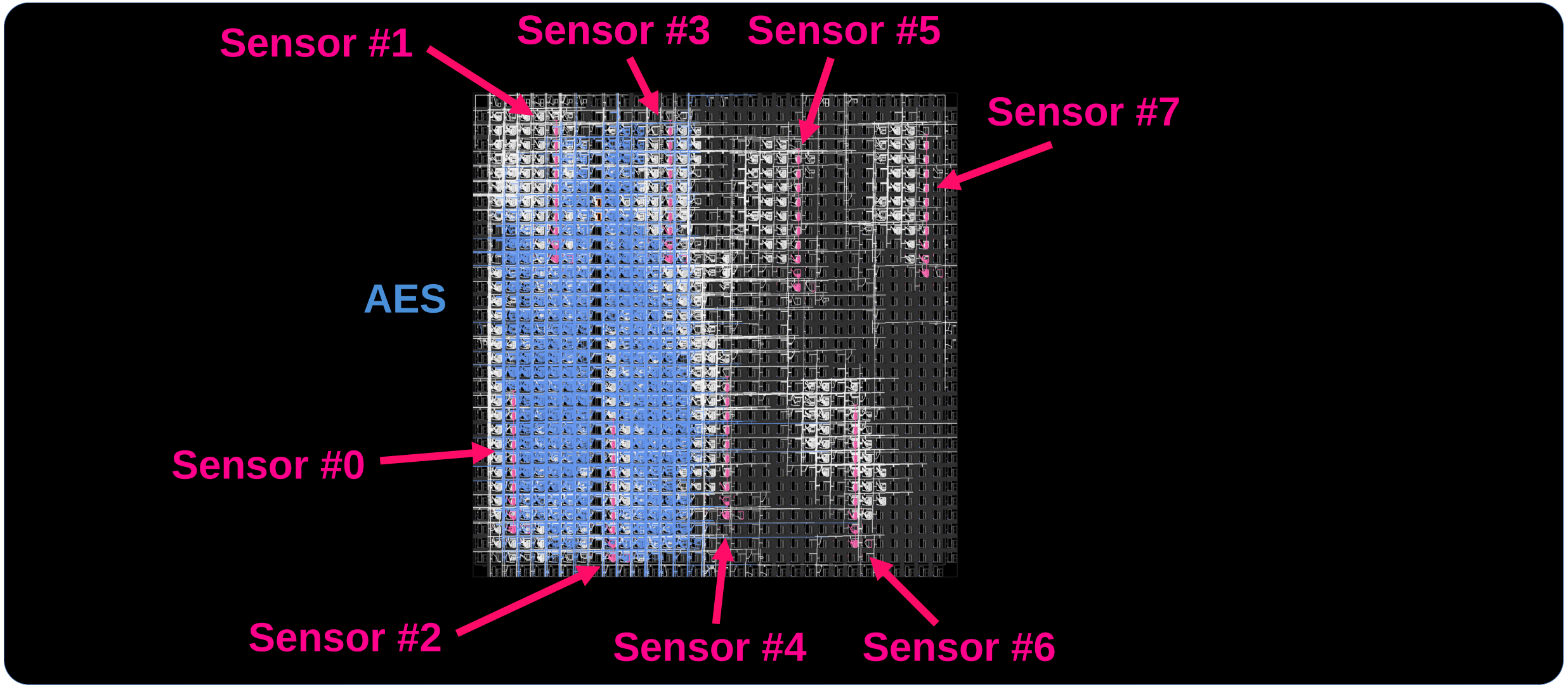
- PCIe FPGA Accelerator
- ~500,000 Logic Elements



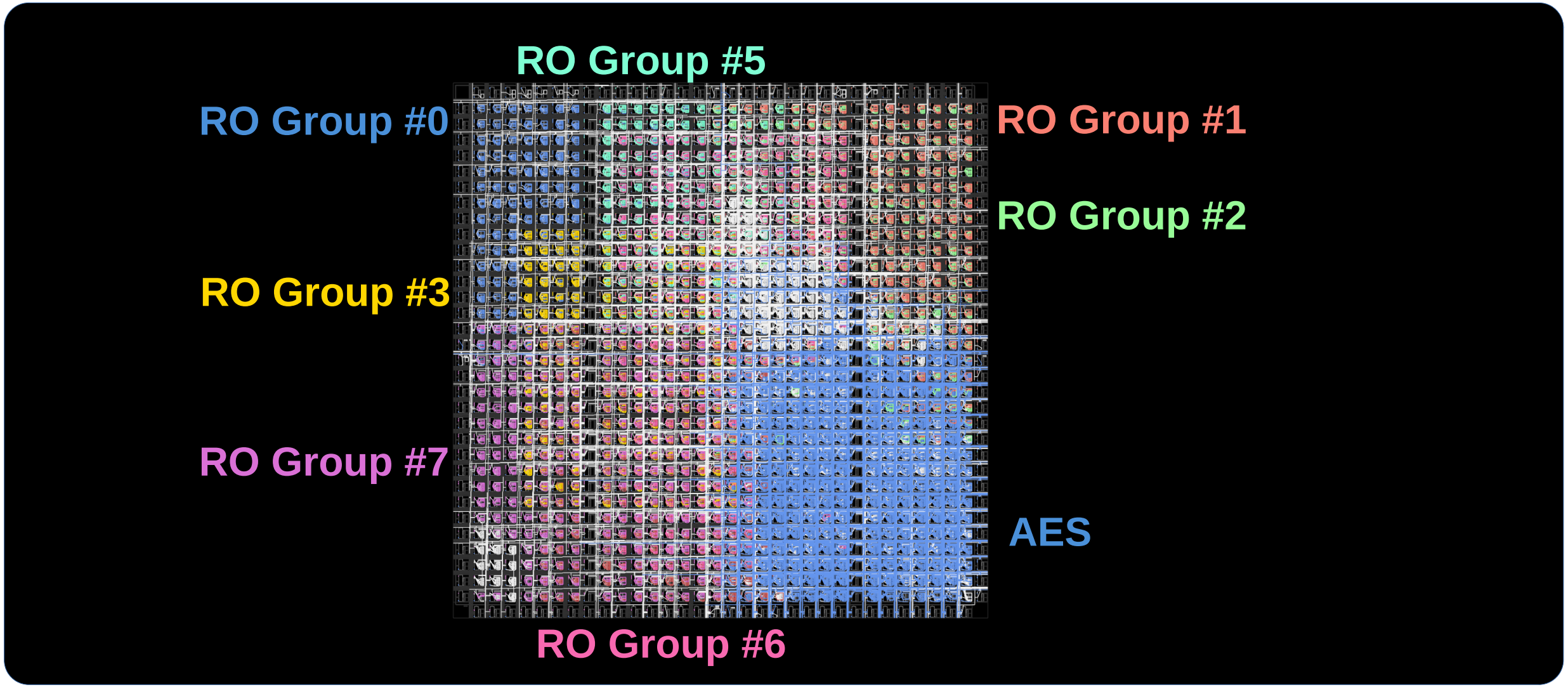
Experimental Part

- Lattice HX8K Breakout Board

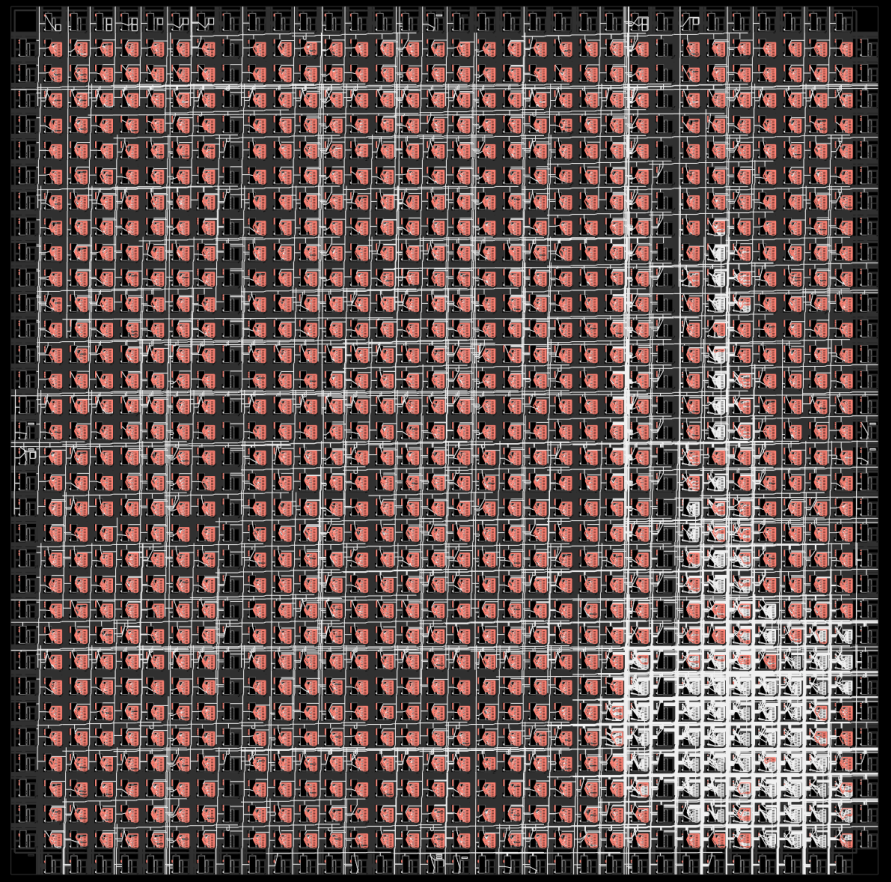
Side-Channel Attack Design



Fault Attack Design



Denial-of-Service (DoS) Design



Ring Oscillators

Blinker Logic

A few Questions and Things to Look At

- SCA:
  - Collect 1000+ traces before taking a detailed look into bytes/bits leakage
  - After switching sensors you might want to reset CPA (or they mix)
  - Q: Do you see a pattern in which bytes leak, and why could that be?
- DFA:
  - Find best parameter combination maximizing usable faults injection
  - Different depending on the board!
- DoS:
  - Look at the LEDs: Two LEDs should be blinking for correct operation
  - Try different boards – not all crash / in same way
  - Try to reset after the crash, and see if it can recover or not

Git for very interested participants ;-) https://git.informatik.kit.edu/i83/security/nessy21