PB173 Domain specific development: side-channel analysis

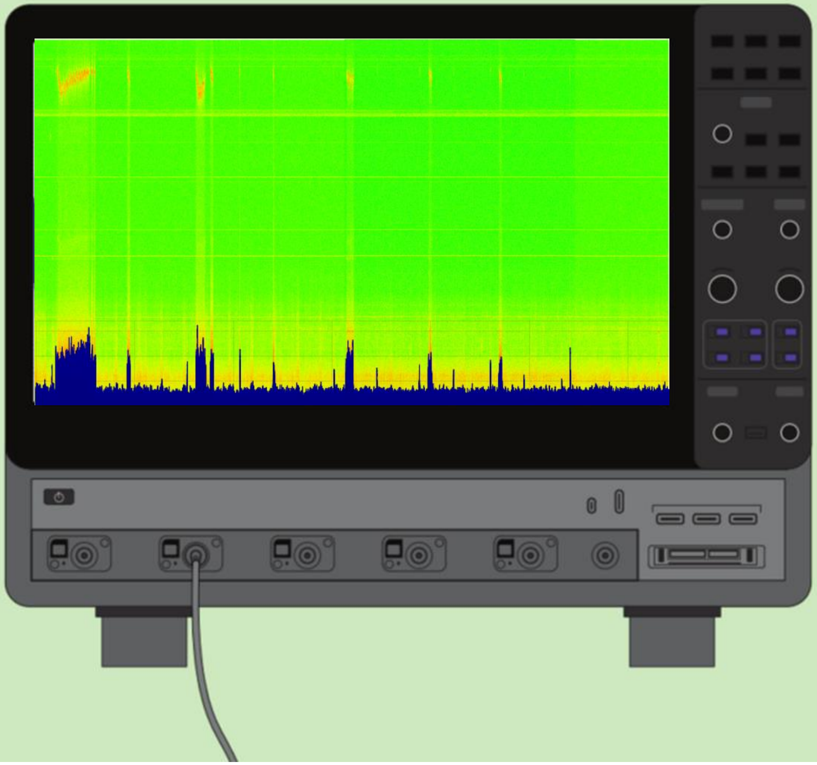
Seminar 4: Various Tasks
Goal → Implementing CPA and DPA

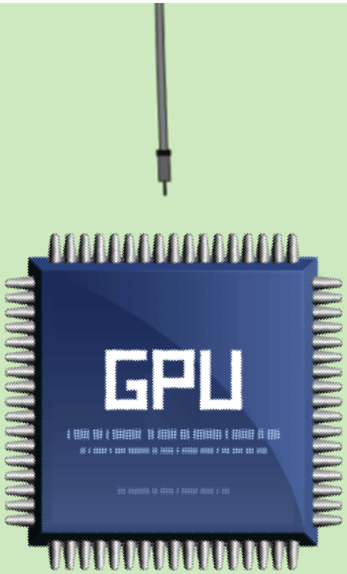
Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

Centre for Research on Cryptography and Security

EXAMPLE: *On Reverse Engineering Neural Network on…*





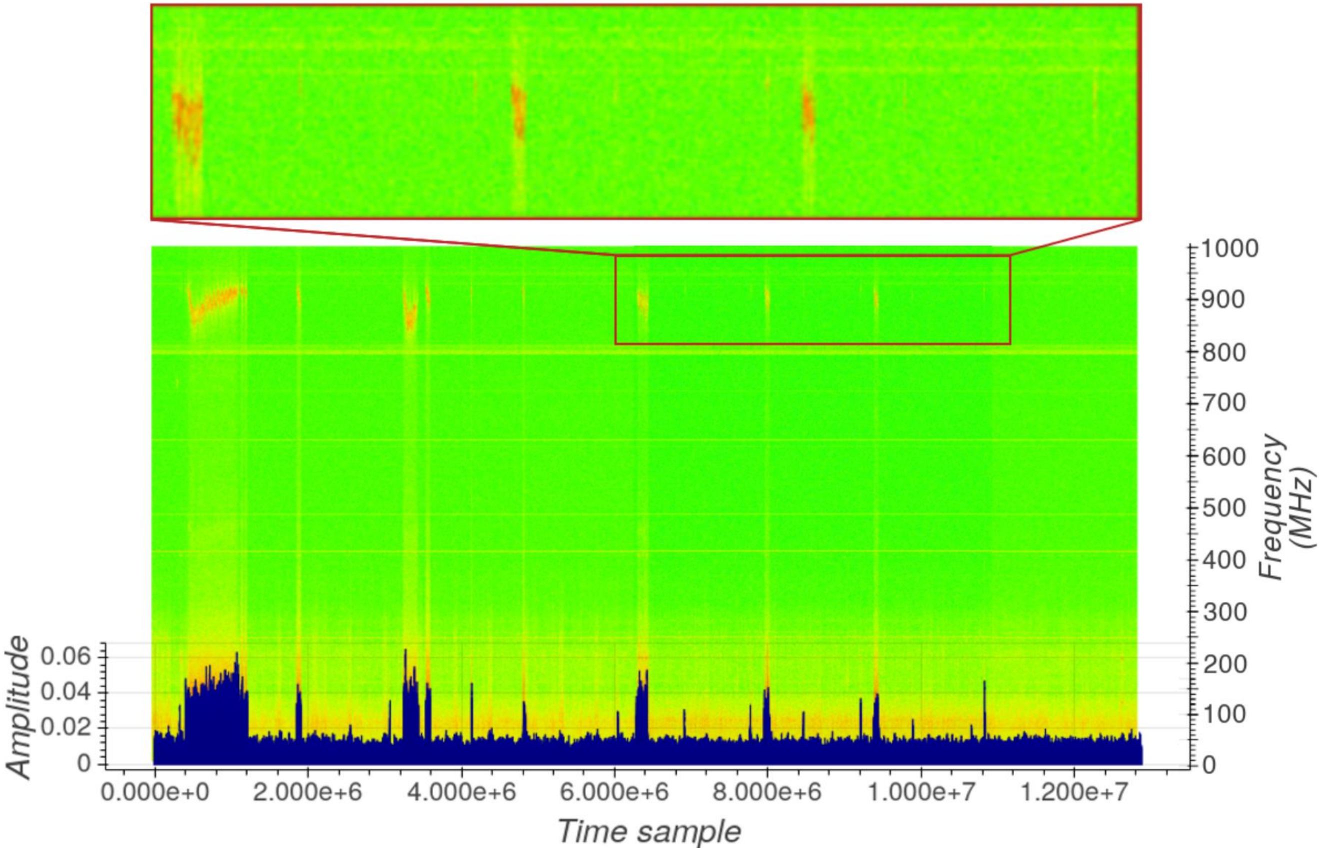
[AIHWS2021]
Łukasz Chmielewski and Léo Weissbart

Radboud University

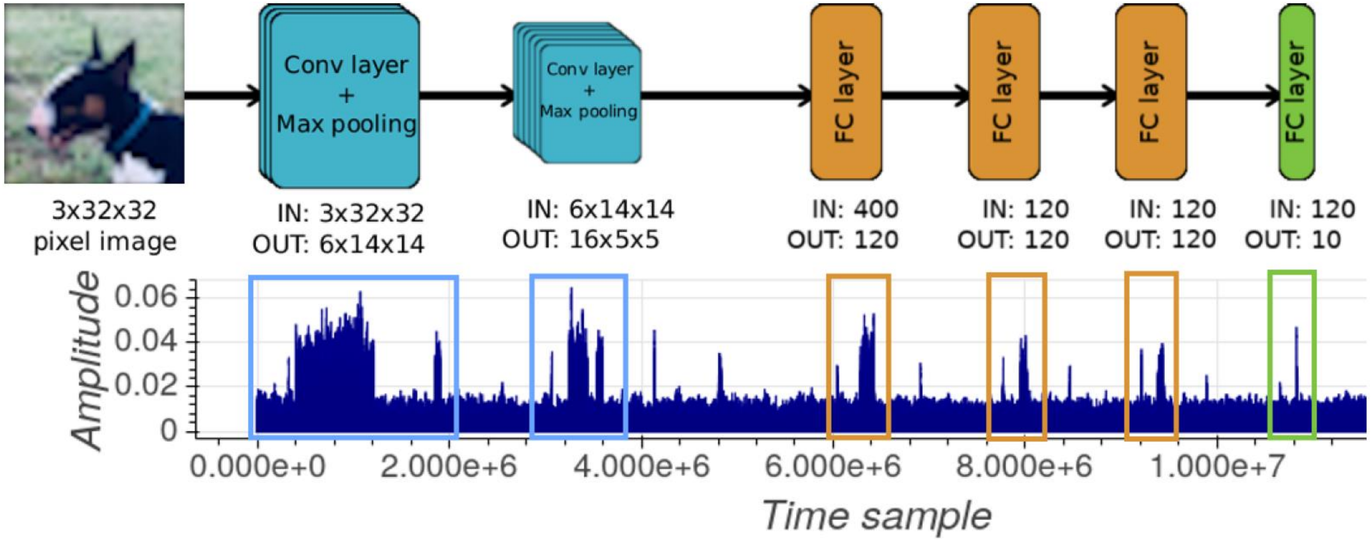
TU Delft
Delft University of Technology

riscure

High Level SPA (Spectrogram)



Reverse Engineering NN on GPU



- Done: all characteristics recoverable with SPA.
- Current work: attacking weights
  - Correlation Power Analysis on float multiplications
  - Deep Learning on Deep Learning
  - Template Attacks on Deep Learning
- Goal: finish this year!

- Cooperation: Léo Weissbart, Péter Horváth, and Lejla Batina

Catch-up

- Looking at the traces:
  - See the new script in the Seminar04 folder

- Have you installed ChipWhisperer?
  - If not then I can try to help.
- What about homework?
  - Where have you got?

Task 1: modify the code

- Modify the code
- Find where the code is
- Enable ADD_JITTER
- See the traces
- What do you think is happening?
- If you have time:
  - try to reduce the number of AES rounds

Task 2: Correlation

- Did anyone run it before?
- Try to correlate all input bytes and output bytes
- What does it mean what we see?
- Where is crypto performed?

Task 2: Input Output Correlation

- Did anyone run it before?
  - This is not the most efficient version of code ☺
  - Try to explain the code
- Try to correlate all input bytes and output bytes
- What does it mean what we see?
- Where is crypto performed?

Task 3: Input Output DoM

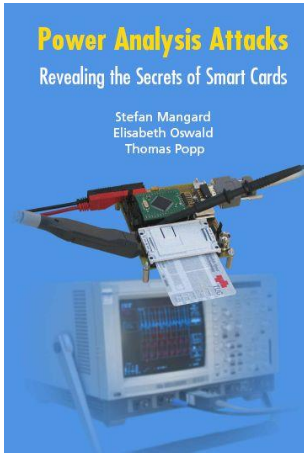
- Try to compute the difference of means for all bits:
  - 128 bits of input
  - 128 bits of output
- What does it mean what we see?
- Where is crypto performed?

Task 3: Correlation Power Analysis Attack

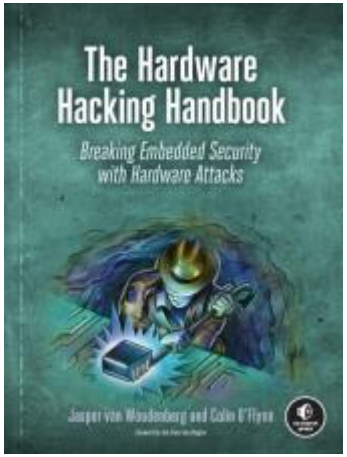
- Try to implement it based on the code and the cells provided
- If you manage then try Difference of Means

Reading

- For interested people
- Side-Channel Analysis – blue book:
  - http://dpabook.iaik.tugraz.at/
  - The books is available at the uni.
  - Look online



- The Hardware Hacking Handbook:
  - https://nostarch.com/hardwarehacking
  - I have an epub version.


The Hardware Hacking Handbook
Breaking Embedded Security with Hardware Attacks
Jasper van Woudenberg and Colin O'Flynn

Questions