PB173 Domain specific development: side-channel analysis

Seminar 6: First Steps & CPA and DPA

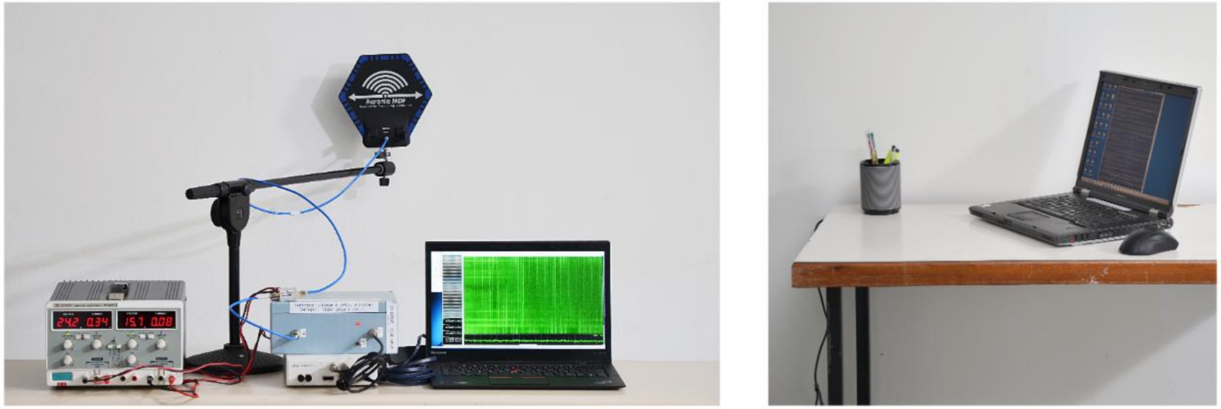
Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

Centre for Research on Cryptography and Security

Example: Practical TEMPEST for $3000

- ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs
  - https://eprint.iacr.org/2016/129.pdf
- E-M trace captured (across a wall)

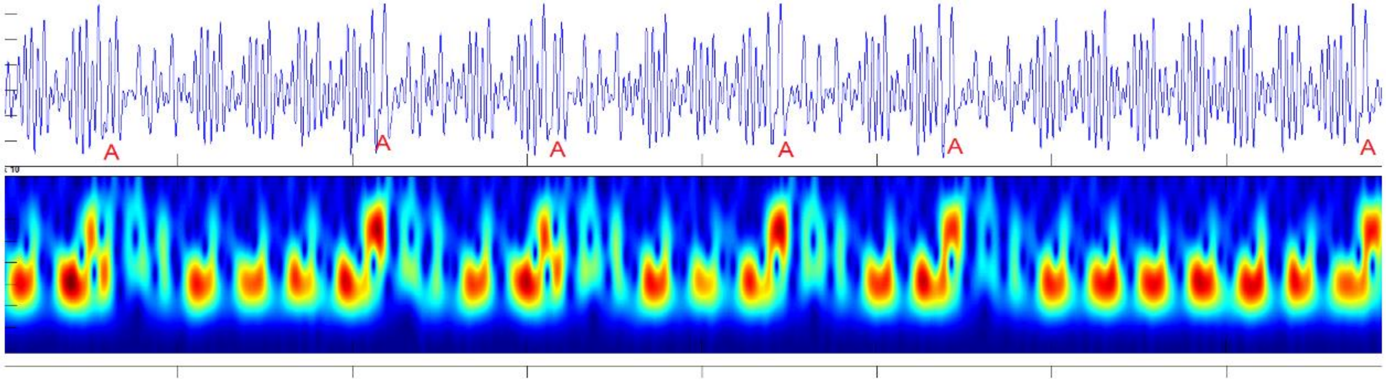


(a) Attacker's setup for capturing EM emanations. Left to right: power supply, antenna on a stand, amplifiers, software defined radio (white box), analysis computer.

(b) Target (Lenovo 3000 N200), performing ECDH decryption operations, on the other side of the wall.

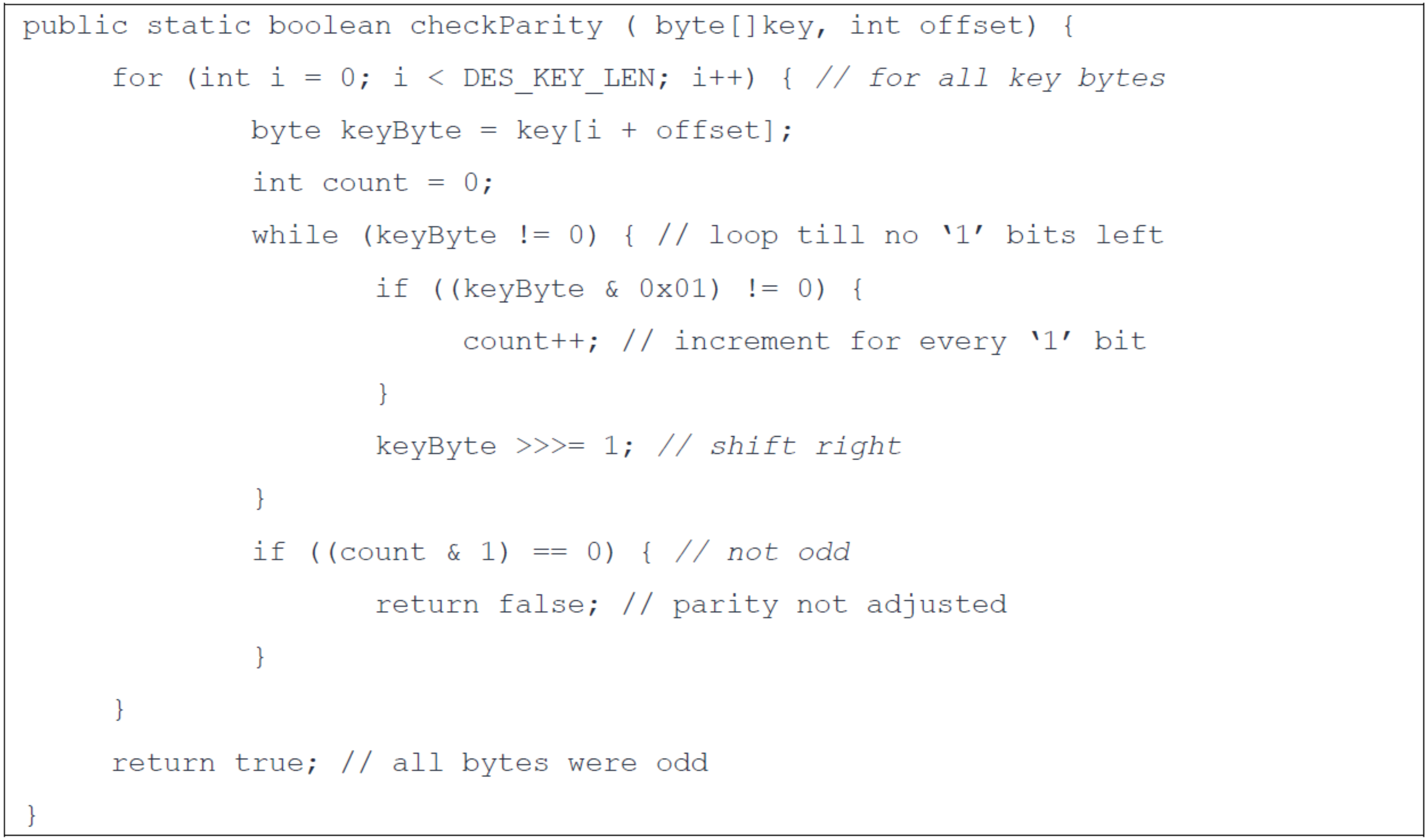
Example: Practical TEMPEST for $3000

- ECDH implemented in latest GnuPG's Libgcrypt
- Single chosen ciphertext – used operands directly visible



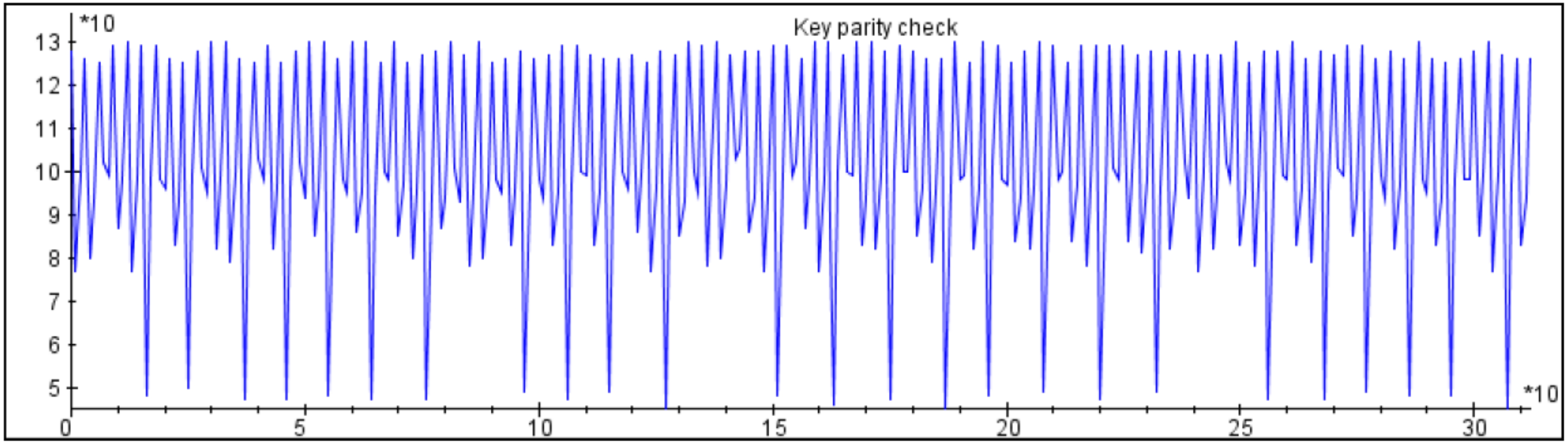
Finishing DES Parity Fail:

What is wrong here?



```
public static boolean checkParity ( byte[]key, int offset) {
    for (int i = 0; i < DES_KEY_LEN; i++) { // for all key bytes
        byte keyByte = key[i + offset];
        int count = 0;
        while (keyByte != 0) { // loop till no ‘1’ bits left
            if ((keyByte & 0x01) != 0) {
                count++; // increment for every ‘1’ bit
            }
            keyByte >>>= 1; // shift right
        }
        if ((count & 1) == 0) { // not odd
            return false; // parity not adjusted
        }
    }
    return true; // all bytes were odd
}
```

???


Key parity check
*10
13
12
11
10
9
8
7
6
5
*10
0
5
10
15
20
25
30

???

???

Groups

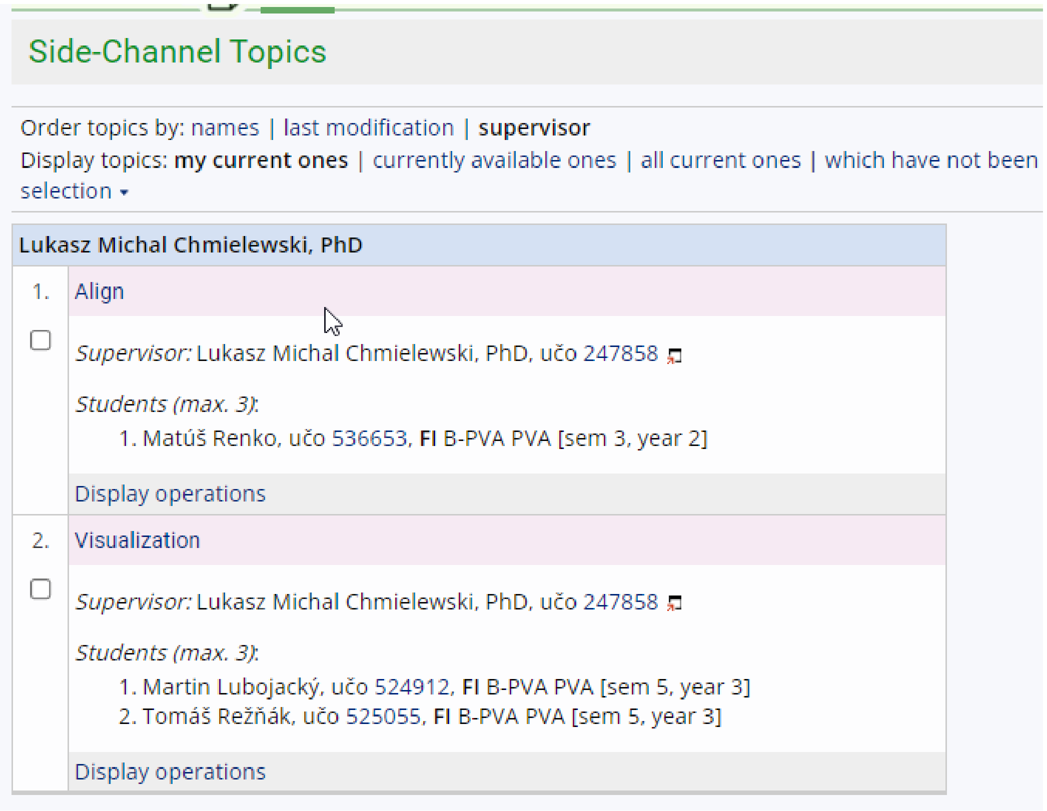
- Currently 3 groups (3+3+3)
- Weekly Code Development based on discussions.
  - Uploading code to GitHub. Everyone needs to commit!
  - Languages: Python, Julia, any
- Topics:
  - Standard Signal Processing, Alignment, Visualization, Efficient Attacks (CPA & DPA), Efficient Parallel Acquisition with ChipWhisperer, Signal Processing for Public Key Crypto.
- I will go through each group topic and discuss what to do.
- Then I will help later on.

Division

- Group 1: Tomas Re, Tomas Ro, Martin
  - Topic: Visualization
  - GitHub repository: -, please create
- Group 2: Michael T, Lubomir, Richard
  - Topic: Standard Processing
  - Do you still think about the topic 5?
  - GitHub repository: +
- Group 3: Michal, Matus, Filip
  - Topic: Align
  - GitHub repository: +
- Extra people?

Organization

- Please register in IS:



Side-Channel Topics

Order topics by: names | last modification | **supervisor**
Display topics: **my current ones** | currently available ones | all current ones | which have not been selection ▾

Lukasz Michal Chmielewski, PhD

1. Align

□ *Supervisor:* Lukasz Michal Chmielewski, PhD, učo 247858

Students (max. 3):
1. Matúš Renko, učo 536653, **FI** B-PVA PVA [sem 3, year 2]

Display operations

2. Visualization

□ *Supervisor:* Lukasz Michal Chmielewski, PhD, učo 247858

Students (max. 3):
1. Martin Lubojacký, učo 524912, **FI** B-PVA PVA [sem 5, year 3]
2. Tomáš Režňák, učo 525055, **FI** B-PVA PVA [sem 5, year 3]

Display operations

Group 3: Alignment

- Goals:
  - Correlation-based Alignment
  - Peak-Based Alignment
  - Optional: elastic versions
- Look at: AES_fixed_rand_input_CAFEBABEDEADBEEF0001020304050607+SAVEEVEN(0,1000)+MIS(100).trs
- First tasks:
  - investigate cross-correlations in python
  - See all the uploaded scripts
  - Especially SaveAs.py and correlation.py
- Main task – I will explain on the whiteboard.

Group 2: Visulation

- Displaying Traces
- Manual Manipulation of the traces
- Continuously investigating different traces

- First Task: implement displaying traces using 2-3 different libraries
  - Matplotlib, bokeh, search for more
  - Someone did some work on that. Have a look here, but it might be chaotic: https://github.com/nilswiersma/pywf/tree/master
- Main task – I will explain on the whiteboard.

Group 1: Standard Signal Processing

- Averaging, Standard Deviation
- Spectral Intensity, Spectrum (Frequencies)
- Correlation

- First Tasks:
  - Implement easy modules: average, standard deviation, histogram, absolute value,
  - You can have a look at SaveAs.py and correlation.py
  - Try to implement computing spectrum, some inspiration: https://realpython.com/python-scipy-fft/
- Main task – I will explain on the whiteboard.

Let’s go back to ChipWhisperer

- Open the progress notebook
- Let’s have a look at CPA and DPA

CPA explained on the example:

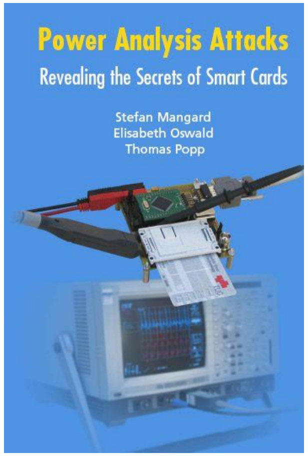
- https://github.com/newaetech/chipwhisperer-tutorials/blob/master/courses_sca101_SOLN_Lab%204_2%20-%20CPA%20on%20Firmware%20Implementation%20of%20AES-CWNANO-CWNANO.rst

Let’s discuss your work

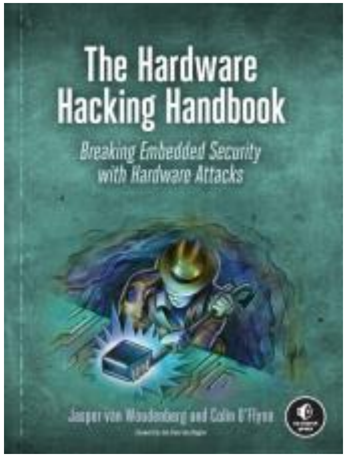
- Work in groups

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