PB173 Domain specific development: side-channel analysis

Seminar 5: Traces Investigation, Projects Division, & Going on with Implementing CPA and DPA

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

CROCS
Centre for Research on Cryptography and Security

Catch-up

- How is going your work with Chip Whisperer / CPA?
  - https://www.youtube.com/watch?v=pPy1vgpEyJA
  - Excercise_CPA_DPA_prog3.ipynb ?
- Should I go through that again?
  - 10 min now?

Outline

- **Projects Division**:
  - Groups
  - Topics Selection
  - First tasks

- Traces Analysis
  - Looking at some new traces
- Finalizing ChipWhisperer with CPA
- Kyber demo/presentation
- (Simple) Homework

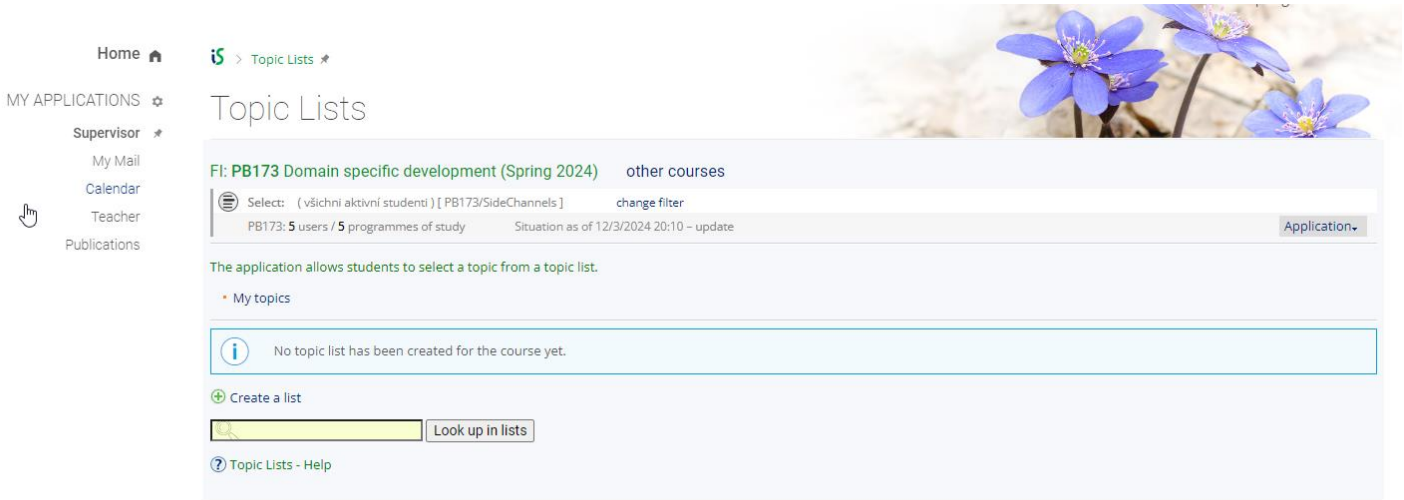
GROUPS AND PROJECTS

Groups Division (beginning)

- Could you divide into 2 groups?
  - 3 + 2 ? I will take into account the size of each group.
  - If someone prefers to be alone, then we can have three groups.
  - Divide before the next seminar.
- I will propose five topics, and you will choose them.
  - Decide before the next seminar.
  - In case of conflicts: Rock, Paper, Scissors.
- Regular development-based 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.
    Disclaimer: not all topics have been introduced well yet.

Organization

- Create GitHub Repository per group.
- On my side, after you choose the topics I will organize them in IS:



Divide (we will fill it in during the next seminar)

- Group 1:
  - Topic:
- Group 2:
  - Topic:
- Group 3?:
  - Topic:

1: Standard Signal Processing

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

- First Task: implement a few easy ones manually
- Subsequent tasks: experiment with different libraries

2: Alignment

- Correlation-based Alignment
- Peak-Based Alignment
- Optional: elastic versions
- …

- First Task: investigate cross-correlations in python
- Subsequent tasks: implement naïve correlation based-alignment

3: Vizulation

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

- First Task: implement displaying traces using 2-3 different libraries
- Subsequent tasks: investigate the possibility of manual modifications while displaying the traces

4: Correlation / DPA

- Efficient and Memory Friendly Implementation of DPA and CPA
- Different Models
- Incremental Correlation
- …

- First Task: implement CPA and DPA in python
- Subsequent tasks: implement incremental correlation in python or Julia (or C), you can use a library

5: Parallel computations with acquisition

- Implement multithreaded Acquisition + Processing
- Measure Efficiency
- …

- First Task: measure the efficiency of the acquisition
- Subsequent tasks: observe the impact of processing and try to add WindowResample in parallel to the acquisition

6: Signal Processing for Public Key Crypto

- How to Divide RSA, ECC traces?
- Correlation-based Extraction
- Peak-based Extraction
- Memory Friendly?
- …

- First Task: investigate cross-correlation
- Subsequent tasks: implement peak-based extraction

Choose the topic

- Which topic would you prefer?
- Do you need some time?
- Let’s discuss the first steps.

TRACE INSPECTION

Task 1: Guess what it is (1)?

- Open the trace acq_full_1_SAVE_0_20.trs
  - and visualize it
- What do you get?
- Observations?
- Try WindowResample
- Modify the parameters

- What it is?
  - How many patterns are there?
- Conclusion?

Task 2: Guess what it is (2)?

- Open the trace acq_full_2_SAVE_0_20.trs
  - and visualize it
- What do you get?
- Any guess in comparison to Task 1?

- How many patterns are there?
- Conclusion?

CHIPWHISPERER AND DPA

Back to ChipWhisperer…

- Let's go on to where we finished last time.
  - Have you finished Excercise_CPA_DPA_prog3.ipynb ?
  - Did you get the key?
  - What is better DPA or CPA?
- If all is done, try to modify your code to compute input and output correlation:
  - With HW and with ID
- If there is time, try to compute the correlation between the attacked intermediate value SBOX($K_0 \oplus I_0$)
  - What is it useful for? Try to think also about efficiency.

15min: if there is interest, then we can spend more on that on the next seminars

KYBER DEMO BY MILAN

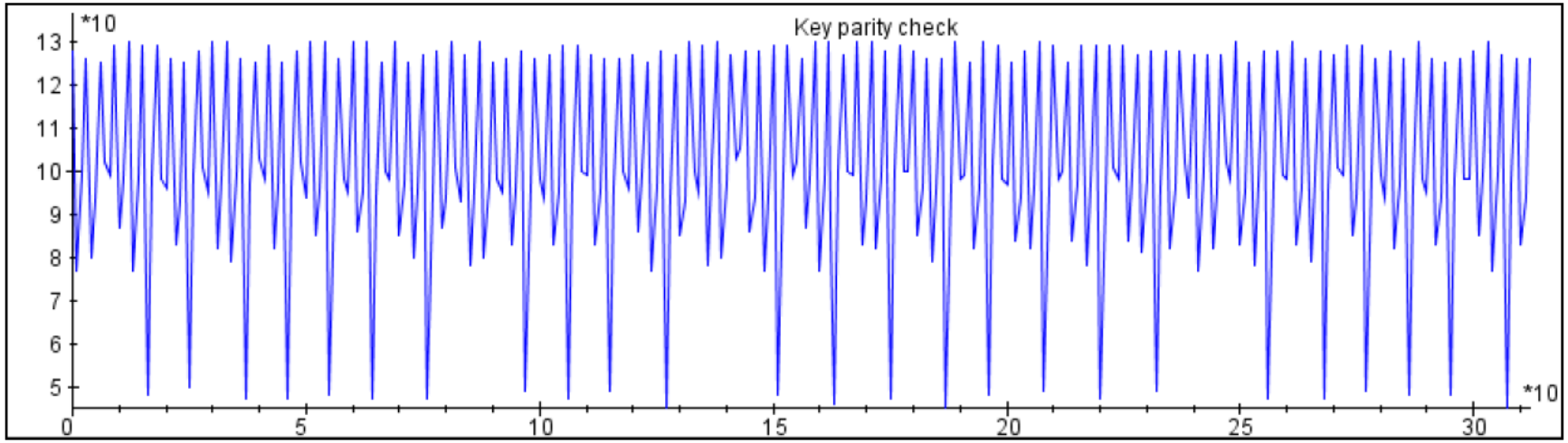
We will spend 5 min on that

HOMEWORK TASK

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
}
```

???

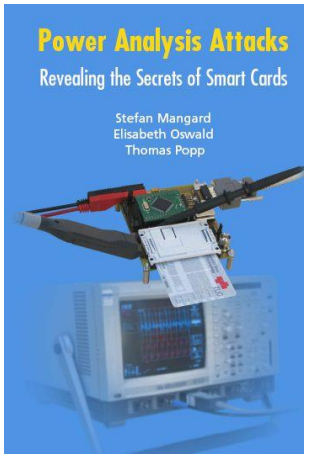

Key parity check
*10
13
12
11
10
9
8
7
6
5
0
5
10
15
20
25
30
*10

???

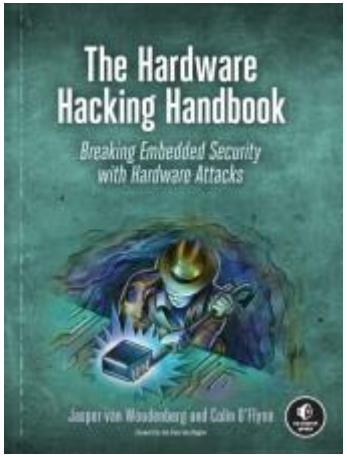
???

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.



Questions