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,

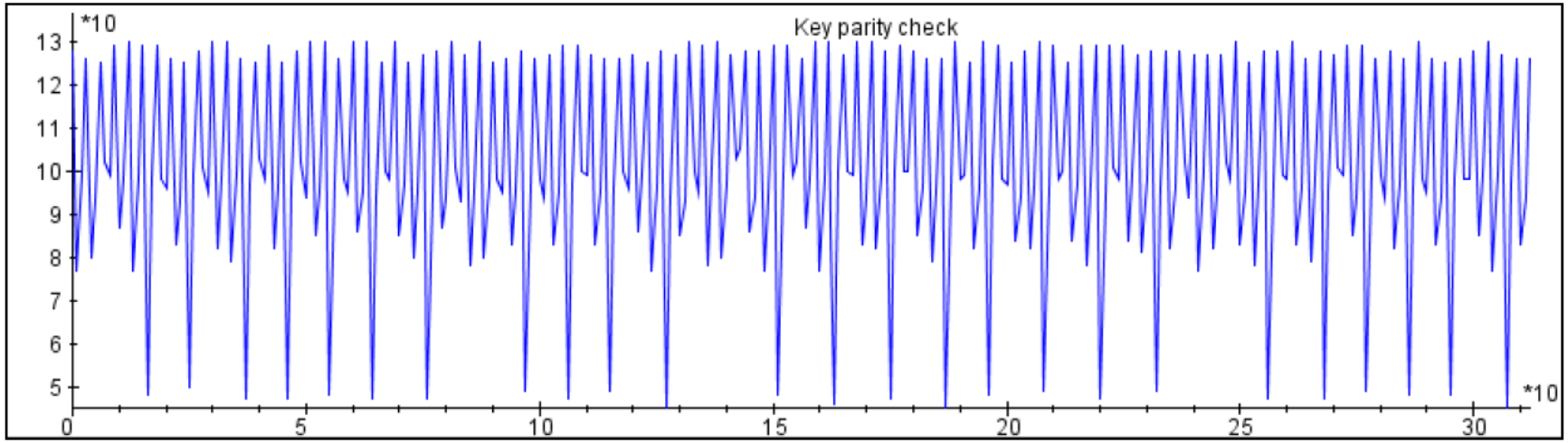
Consultation: A406 Friday 9:00-11:00

CROCS
Centre for Research on Cryptography and Security

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

???

???

Catch-up

- Looking at the traces continued:
  - See the new scripts and traces in the Seminar05 folder.
  - Use previous traces.
- Have you installed ChipWhisperer?
  - If not then I can try to help.
  - I have VM with me.
- Have you got somewhere with CPA?

Outline

- Traces Analysis
  - Continued from last week + new traces
- Projects Division:
  - 4 groups: 3+3+3+2 is it OK with you?
  - Topics Selection
  - First tasks

- Back to ChipWhisperer and CPA

Task 1: AES

- Finish Task from the last seminar:
  - AES_fixed_rand_input_CAFEBABEDEADBEEF000102 0304050607+SAVE(0,20).trs
  - Let’s run WindowResample on that.
  - Experiment with overlab and window and absolute
- Observations

Task 2: 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 3: 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?

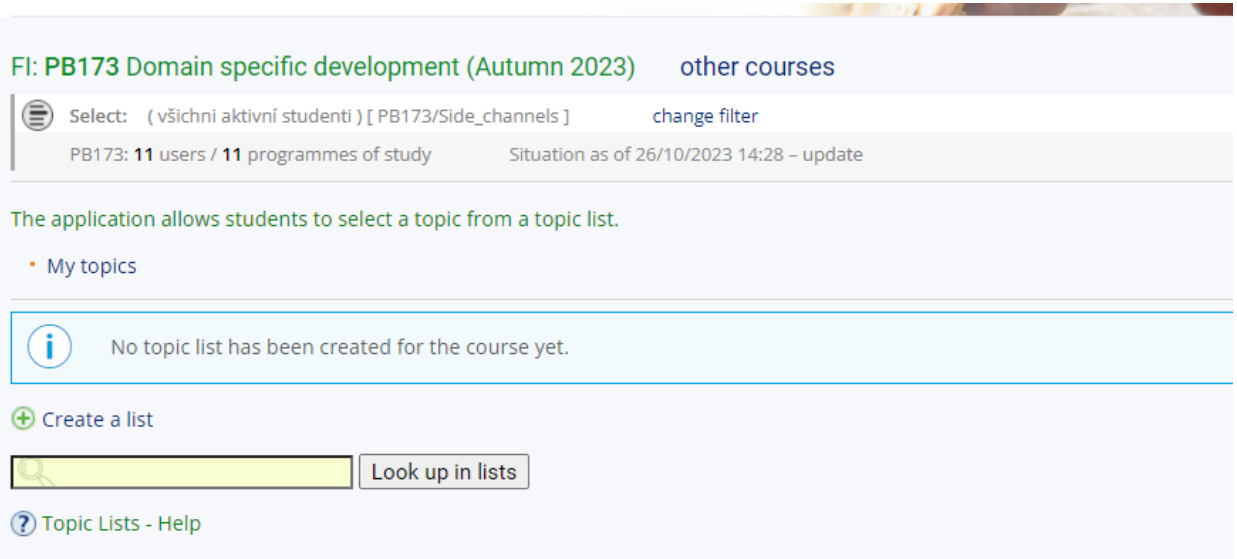
- How many patterns are there?
- Conclusion?

Groups

- Could you divide into 4 groups?
  - 3+3+3+2
  - For the group of 2 people – I will take it into account.
- I will propose five topics and you will choose them.
  - Write on paper.
  - In case of conflicts: Rock, Paper, Scissors.
- 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.

Organization

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



Divide

- Group 1: Tomas Re, Tomas Ro, Martin
  - Topic: Visualization
- Group 2: Michael T, Lubomir, Richard
  - Topic: 1/5
- Group 3: Michal, Matus, Filip
  - Topic: Align

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 and write it on paper

- Write the number of your group
- Give the paper to me

Let’s go back to ChipWhisperer

- Let’s go on to where we finished last time.

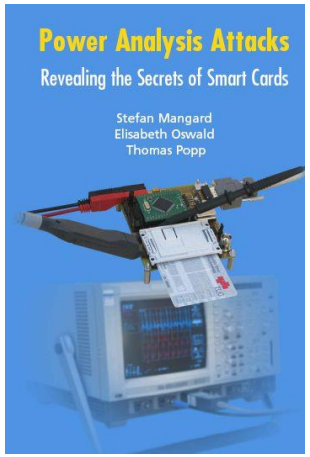
Hint ☺

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

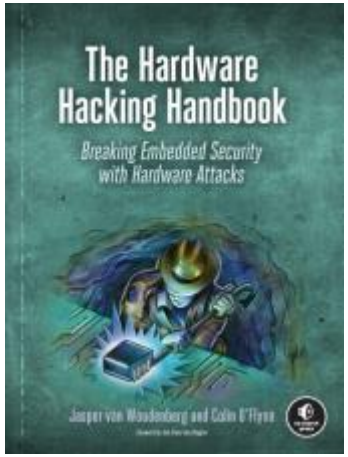
- Try to use the above code in your notebook.
- You can find similar code for DPA.

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