PB173 Domain specific development: side-channel analysis

Seminar 6: Finalizing on First Steps

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00

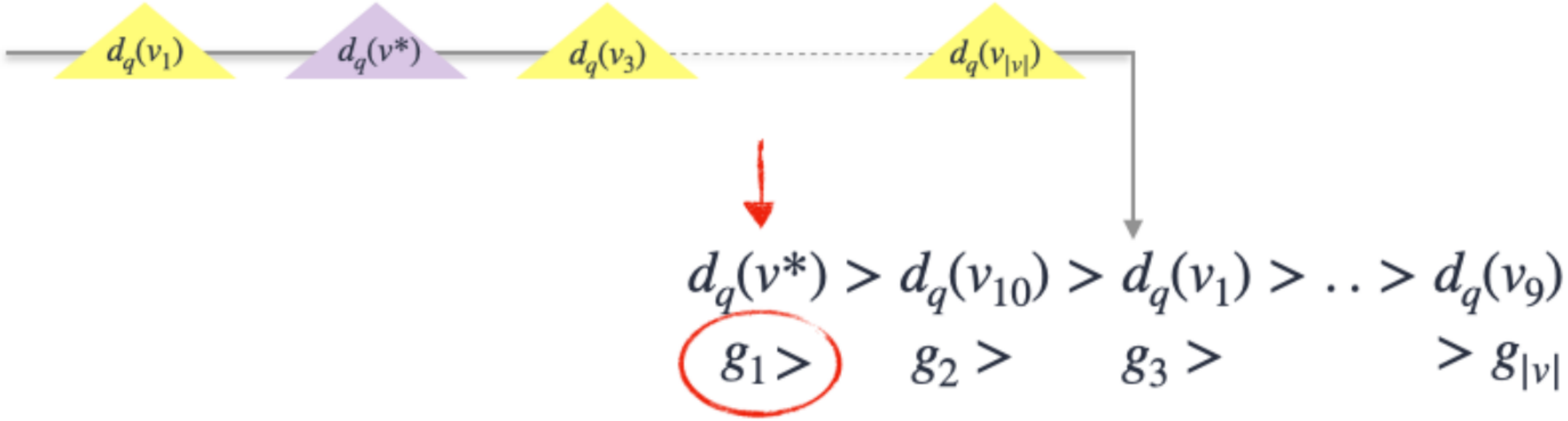
CROCS

Centre for Research on Cryptography and Security

SHORT EXAMPLE

Guessing entropy/Key rank

Lets assume we have the results of a key recovery experiment (DPA or CPA) with q queries/traces. We know that the correct value (e.g., a key byte) is v^*:



$$d_q(v^*) > d_q(v_{10}) > d_q(v_1) > .. > d_q(v_9)$$
$$\boxed{g_1 >} \quad g_2 > \quad g_3 > \quad > g_{|v|}$$

The result is the guess vector:

Position of the correct key candidate = 1

$$g_q = [g_1, g_2, g_3, \dots g_{|v|}]$$

Guessing entropy in the wild

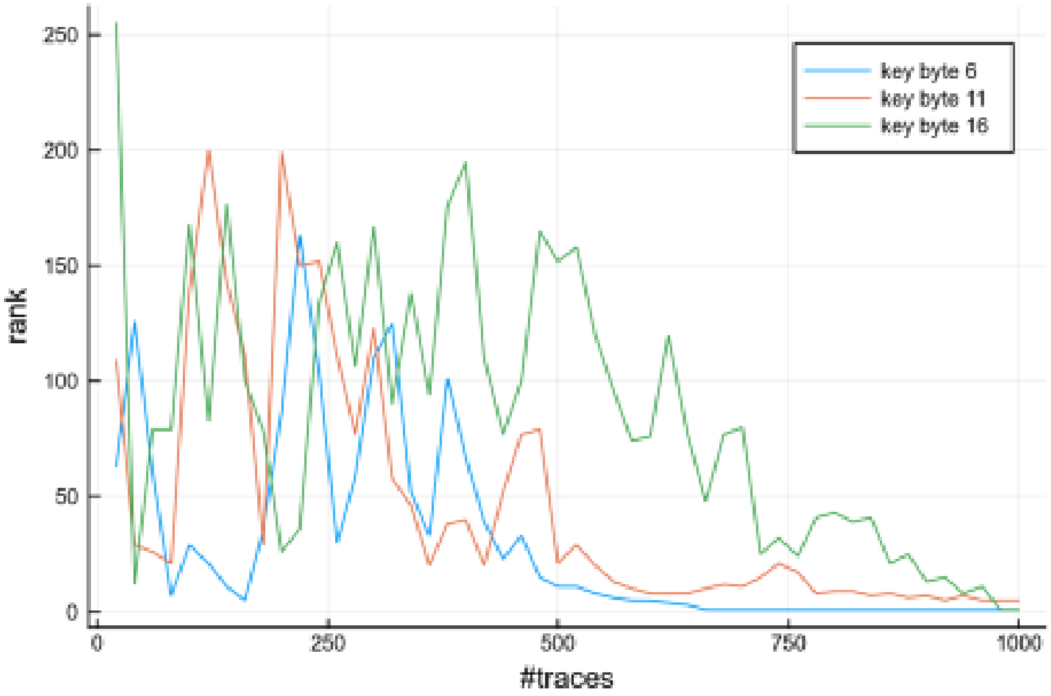


Figure 8: Key rank evolution for hardware AES engine FCA attack.

Source for the figure: Albert Spruyt, Alyssa Milburn, Łukasz Chmielewski, *Fault Injection as an Oscilloscope: Fault Correlation Analysis*, CHES 2020;

Conclusion

- That is all ☺
- Last week DPA actually worked
  - We looked at 0th byte instead of first
- If we have time we will look at another notebook today (see IS)

ORGANIZATIONAL

Final Division

- Group 1: Tomas Re, Tomas Ro, Martin
  - Topic: Visualization
  - GitHub repository: https://github.com/reznakt/pb173-sca-visualization
- Group 2: Michael T, Lubomir, Richard
  - Topic: Standard Processing, Michael might touch also “Parallel computations with acquisition”
  - The group is 3 people since Vendelín left.
  - GitHub repository: https://github.com/LubJur/PB173_standard_signal_processing
- Group 3: Michal, Matus, Filip
  - Topic: Align
  - GitHub repository: https://github.com/mr-akiio/trs-alignment

Reminder: Colloquium

- To get the colloquium
  - You must be present at seminars (2 absences OK)
  - You must be active at seminars (+2 points given by me at the end)
  - **You must submit and get:**
    - **50%: 7 points in total**

      (projects + presentation + activity = 14 points)

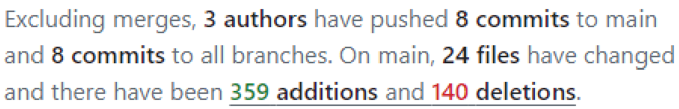
(Modified) Seminars Plan

- 7: today, no points
- **8: evaluation of first steps given last week: 3 points per group (personalized per person based on Github activity) + Giving new tasks**
- 9: Checking Progress: helping & trying to run your tools
- 10: 4 points per group (personalized per person based on GitHub) **+ a short 5-10minuts progress presentation (1 point) +** Giving new tasks
- 11: Checking Progress **[Online]**
- 12: Final seminar: **final short 5-10minuts presentation (1 point) & grading** + grading (2 points for final tasks) + 2 points for activity.

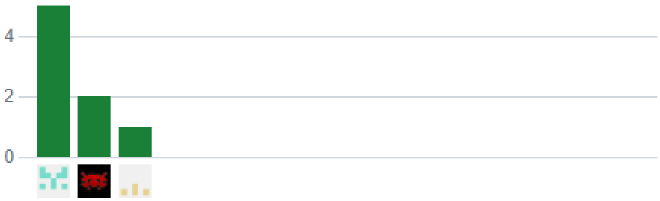
WHAT WAS DONE + GIVING NEW TASKS

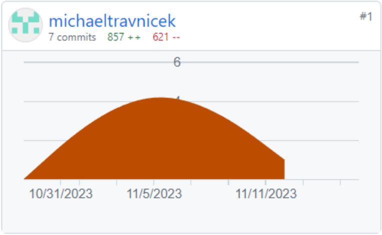
Group 1: Standard Signal Processing

- 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/
- GitHub:

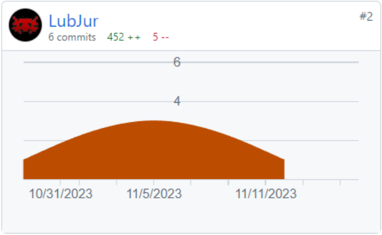


Excluding merges, **3 authors** have pushed **8 commits** to main and **8 commits** to all branches. On main, **24 files** have changed and there have been **359 additions** and **140 deletions**.

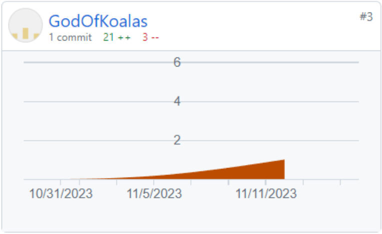




michaeltravnicek #1
7 commits 857 ++ 621 --



LubJur #2
6 commits 452 ++ 5 --



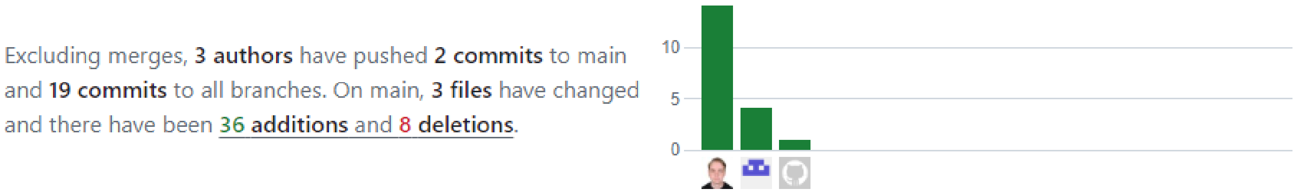
GodOfKoalas #3
1 commit 21 ++ 3 --

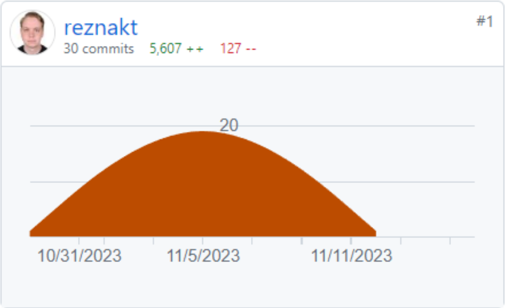
Group 1: Main Goals

- Main Tasks:
  - Spectrogram
  - Incremental Correlation: https://eprint.iacr.org/2022/253.pdf
  - Pipelining
  - Signal-To-Noise Ratio and other metrics

Group 2: Visualization

- First Tasks: 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
- GitHub:


Excluding merges, **3 authors** have pushed **2 commits** to main and **19 commits** to all branches. On main, **3 files** have changed and there have been 36 **additions** and 8 **deletions**.


reznakt
30 commits 5,607 ++ 127 --
#1

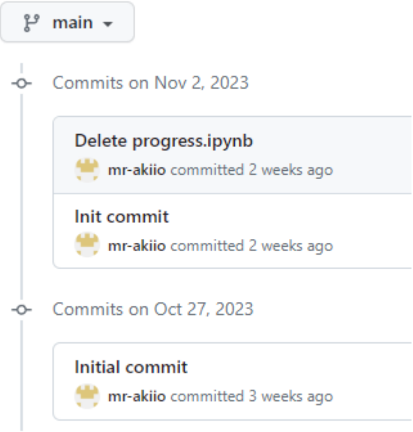
Group 2: Main Goals

- I assume that displaying traces works
  - Multiple traces?
- Main Tasks:
  - Efficiency analysis compared to Matplotlib
  - Moving traces around?
  - Selecting part of the trace to run something (any code)?
  - Try another library?

Group 3: Alignment

- First tasks:
  - investigate cross-correlations in python
  - See all the uploaded scripts
  - Especially SaveAs.py and correlation.py
- GitHub: Insights are disabled so I cannot see statistics. **Please enable it!**

However:



main

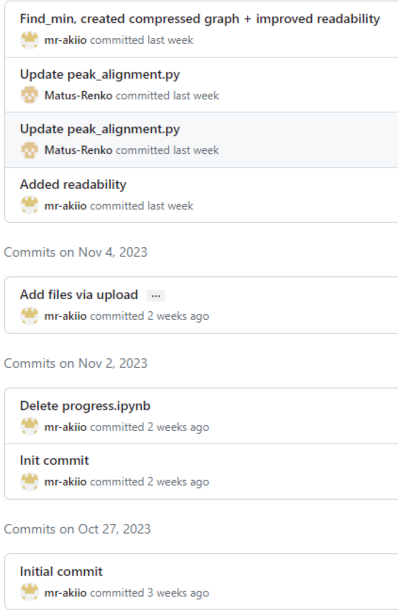
Commits on Nov 2, 2023

Delete progress.ipynb
mr-akiio committed 2 weeks ago

Init commit
mr-akiio committed 2 weeks ago

Commits on Oct 27, 2023

Initial commit
mr-akiio committed 3 weeks ago



Find_min, created compressed graph + improved readability
mr-akiio committed last week

Update peak_alignment.py
Matus-Renko committed last week

Update peak_alignment.py
Matus-Renko committed last week

Added readability
mr-akiio committed last week

Commits on Nov 4, 2023

Add files via upload ...
mr-akiio committed 2 weeks ago

Commits on Nov 2, 2023

Delete progress.ipynb
mr-akiio committed 2 weeks ago

Init commit
mr-akiio committed 2 weeks ago

Commits on Oct 27, 2023

Initial commit
mr-akiio committed 3 weeks ago

Group 3: Main Goals

- I assume that some alignments works
- Main Tasks:
  - Finish Peak-based and Correlation-Based Alignments
  - Improve Efficiency
  - Two from:
    - Trace alignment algorithm for suppressing the clock jitter, see pages 45-50 of: https://ged.biu-montpellier.fr/florabium/jsp/win_main_biu.jsp?nnt=2014MON20039&success=%2Fjsp%2Fwin_main_biu.jsp&profile=anonymous
    - Elastic alignment algorithm or
    - Round Based Alignment

Parallel computations with acquisition

- Michael

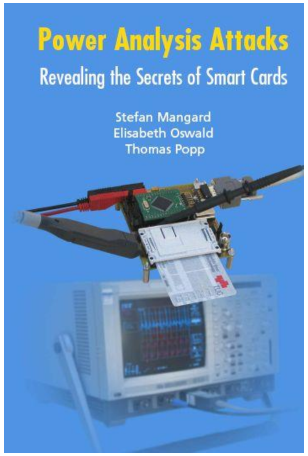
- ?

WALK-AROUND + GRADING

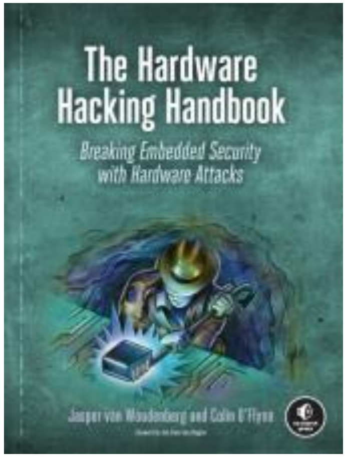
CHIPWHISPER?

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