PB173 Domain specific development: side-channel analysis

Seminar 12: Presentation & Grading (Last Seminar)

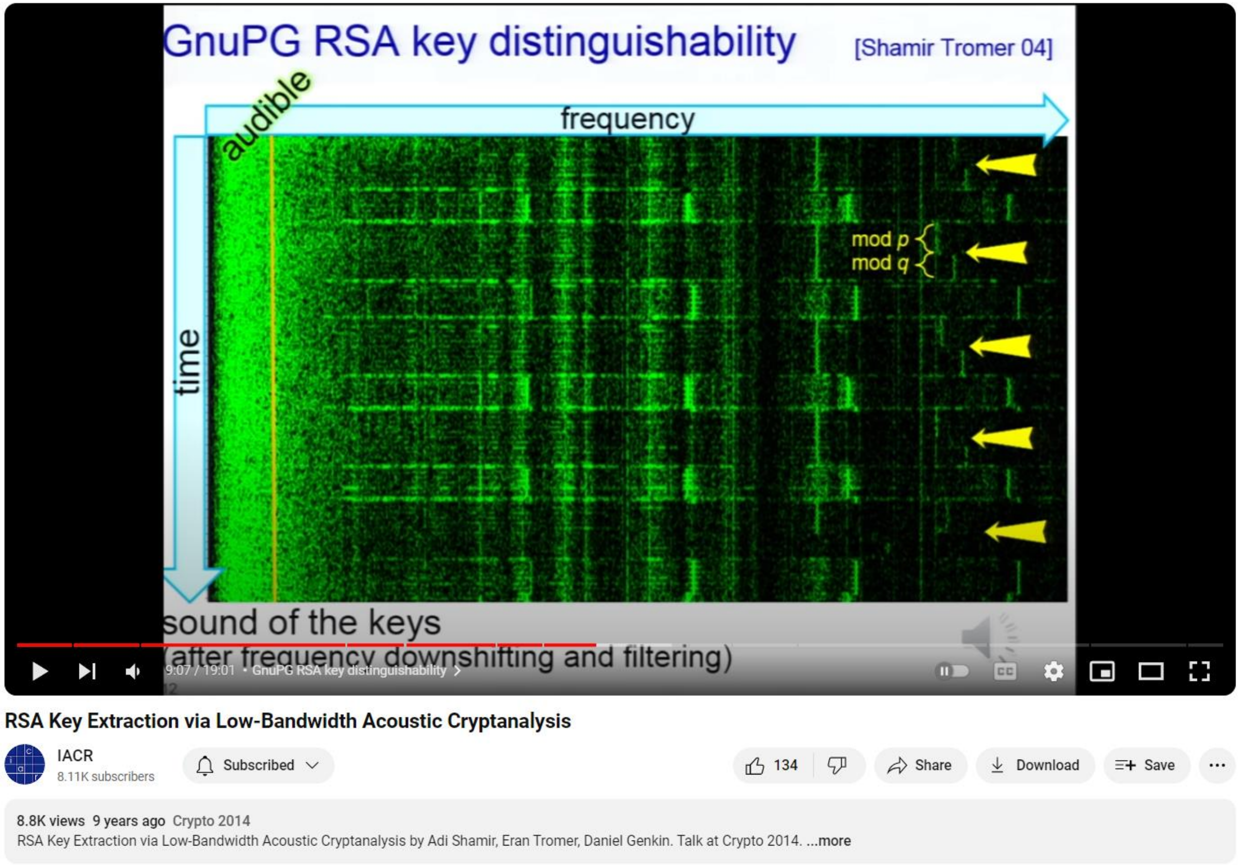
Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Monday 14:00-

CROCS
Centre for Research on Cryptography and Security

ACOUSTIC SIDE-CHANNEL

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis


GnuPG RSA key distinguishability
[Shamir Tromer 04]
audible
frequency
time
mod *p*
mod *q*
sound of the keys
(after frequency downshifting and filtering)
9:07 / 19:01 • GnuPG RSA key distinguishability
Subscribed
134
Share
Download
Save

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

IACR
8.11K subscribers

8.8K views 9 years ago Crypto 2014
RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis by Adi Shamir, Eran Tromer, Daniel Genkin. Talk at Crypto 2014. ...more

- https://www.youtube.com/watch?v=DU-HruI7Q30
- If there is time then we can watch it at the end.

ORGANIZATIONAL

Final Division

- Group 1: Michal, Matus, Filip (?)
  - Topic: Align
  - GitHub repository: https://github.com/mr-akiio/trs-alignment
- 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: Tomas Re, Tomas Ro, Martin
  - Topic: Visualization
  - GitHub repository: https://github.com/reznakt/pb173-sca-visualization

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: 3 points per group (personalized per person based on GitHub) + a short 5-10minuts progress presentation + demo (1 point) + Giving new tasks
- 11: Checking Progress [Online]
- 12: Final seminar: **final short 5-10minuts presentation** (**1** point) & **grading** + grading (**3** points for final tasks) [done after the seminar] + **2** points for activity [comment now publish later on].

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)

SUMMARY & PRESENTATION

Group 1: Main Goals

- Main Tasks:
  - Test more peak-based alignment
  - 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

Group 1: Based on the presentation

Primary:

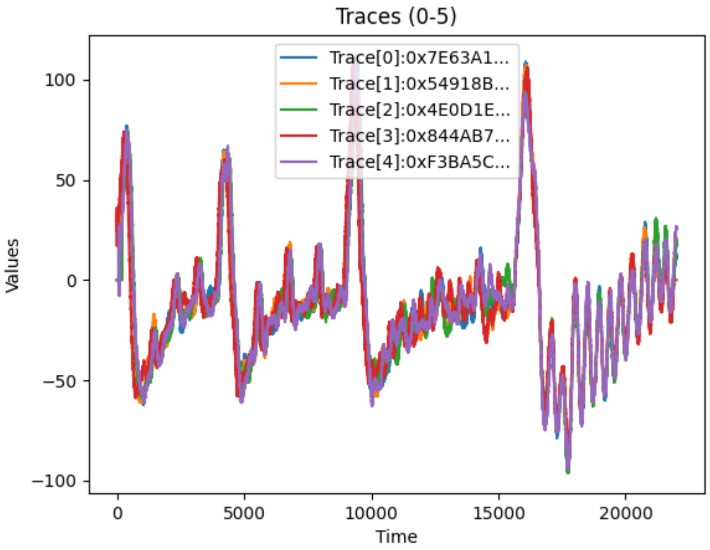
- Peak-Based Alignment
- Correlation-based Alignment
- Investigate cross-correlations in python
- Improve Efficiency

Extra:

- Solving issues: Cross-correlation
- Secondary (first solve issues): Elastic alignment algorithm or Round Based Alignment

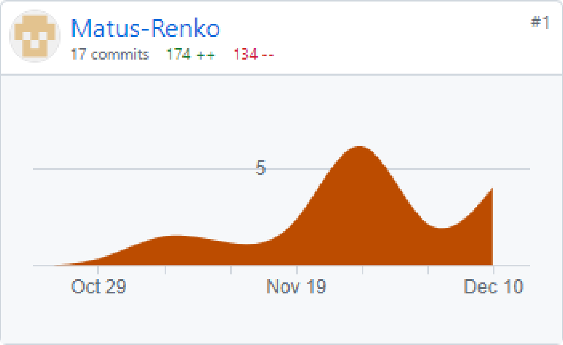
Group 1: Installation and Running

- https://github.com/mr-akiio/trs-alignment
- Installation: all good
- No individual instruction for modules
- Modules work so so but correlation seems to work (?):



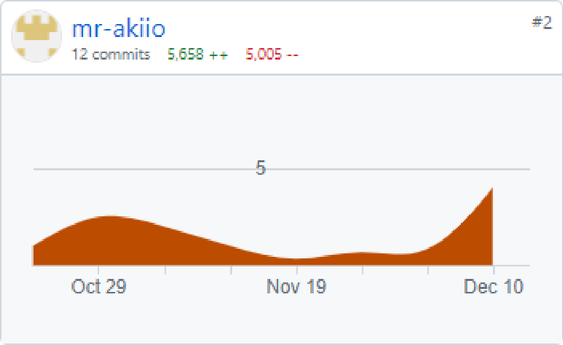
- Well done!
- You did not touch on efficiency (?)
- What is the status of other methods?

Group 1: Work Division



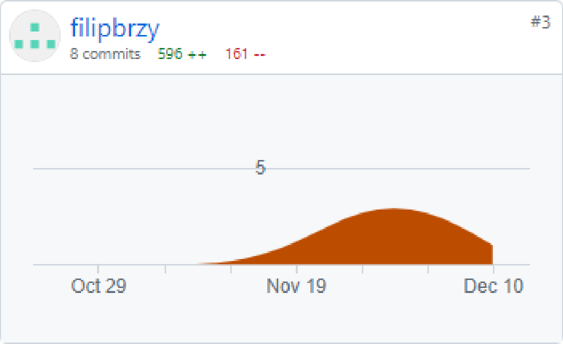
Matus-Renko #1

17 commits 174 ++ 134 --



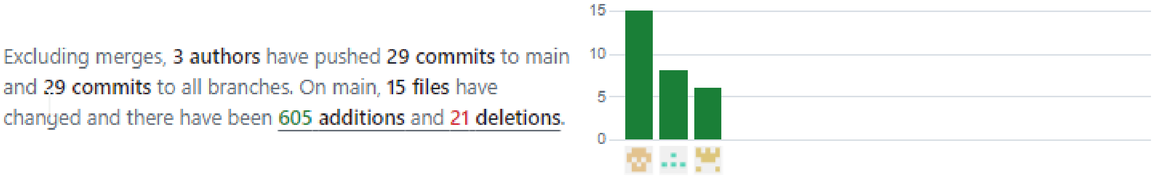
mr-akiio #2

12 commits 5,658 ++ 5,005 --



filipbrzy #3

8 commits 596 ++ 161 --



Excluding merges, **3 authors** have pushed **29 commits** to main and **29 commits** to all branches. On main, **15 files** have changed and there have been 605 **additions** and 21 **deletions**.

Group 2: Main Goals

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

Group 2: based on the presentation

Primary

- Pipelining
- Average, Histogram
- Standard Deviation, Signal-to-Noise ratio

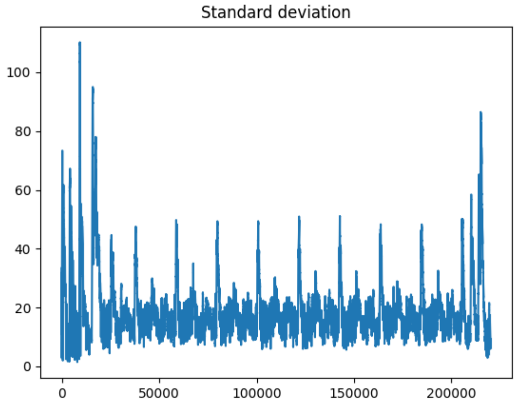
Work in progress:

- Bandpass filter: try to implement it using:
  - https://scipy-cookbook.readthedocs.io/items/ButterworthBandpass.html
- Fourier transform:
  - add an “x” axis with frequencies based on the provided sampling rate.
- check spectrogram
- check transposition
- Check how FFT looks on all traces

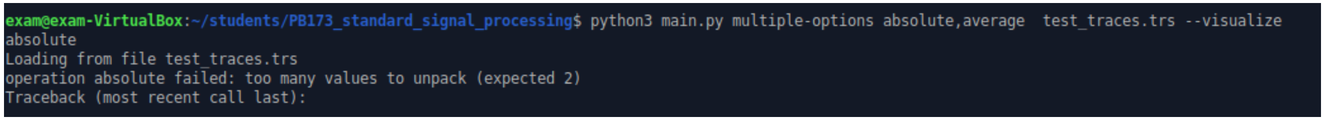
Anything more?

Group 2: Installation and Running

- https://github.com/LubJur/PB173_standard_signal_processing
- Installation: pydantic missing, but all ok



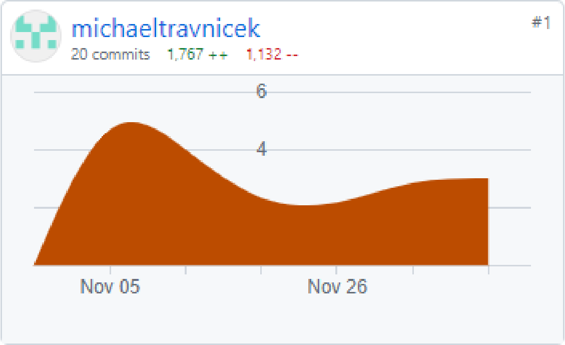
- Overall well done!
- Multiple options failed, probably abs:



```
exam@exam-VirtualBox:~/students/PB173_standard_signal_processing$ python3 main.py multiple-options absolute,average  test_traces.trs --visualize
absolute
Loading from file test_traces.trs
operation absolute failed: too many values to unpack (expected 2)
Traceback (most recent call last):
```

- Can you show me multi-threaded example?

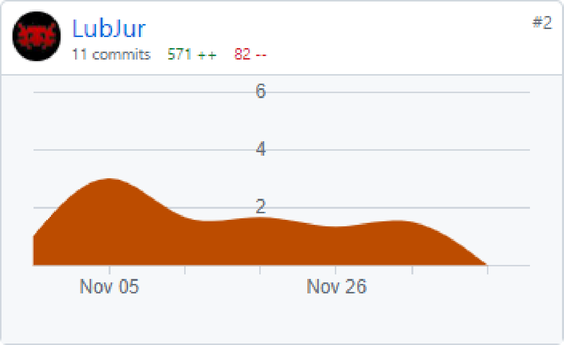
Group 2: Work Division



michaeltravnicek

20 commits 1,767 ++ 1,132 --

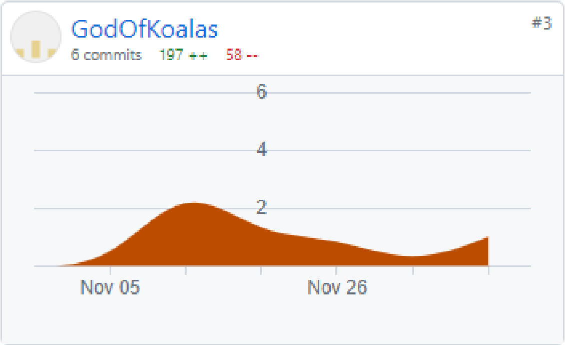
#1



LubJur

11 commits 571 ++ 82 --

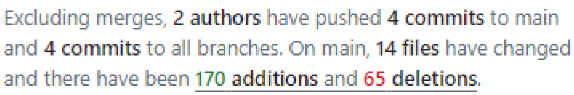
#2



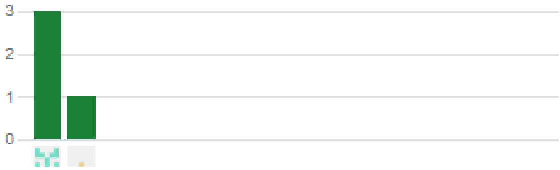
GodOfKoalas

6 commits 197 ++ 58 --

#3



Excluding merges, **2 authors** have pushed **4 commits** to main and **4 commits** to all branches. On main, **14 files** have changed and there have been **170 additions** and **65 deletions**.



Group 3: Main Goals

- Main Tasks:
  - Displaying Traces
  - Moving traces around?
  - Selecting part of the trace to run something (any code)?
  - Comparison to other libraries

Group 3: based on the presentation

Main tasks that are done:

- No backend – the app works in the browser without any setup
- Visualizing traces, dragging them around
- Upload progress bar, Automatically deployed to GitHub Pages

Things to do:

- Working in-app parser for .trs files
- Setting for which traces to visualize
- Working Ctrl+Z for trace dragging

Secondary:

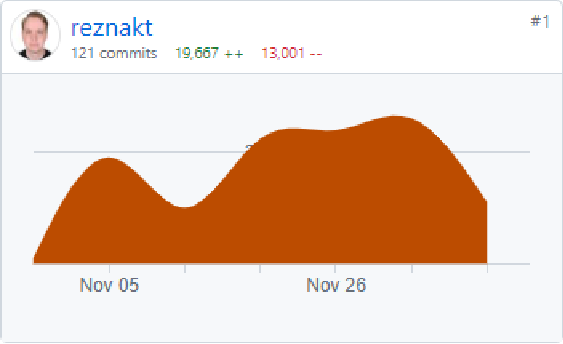
- Parse and apply more parameters from the TRS files (sample rate…)

Group 3: Installation and Running

- Installation ok
- Running natively in a browser – works great! It seems very smooth.
- Trs formal seems supported.

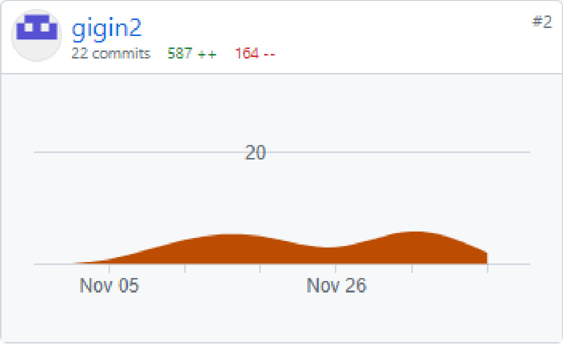
- Overall, great work!
- Can I use it in the lectures/seminars?

Group 3: Work Division



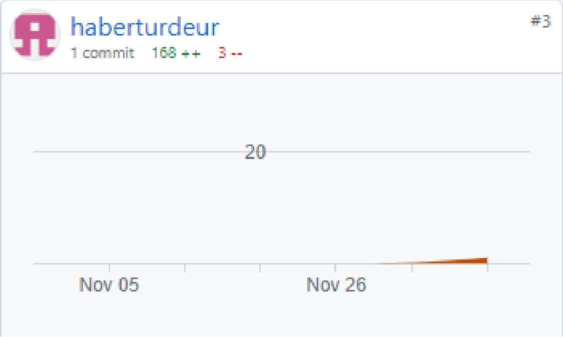
reznakt #1

121 commits 19,667 ++ 13,001 --



gigin2 #2

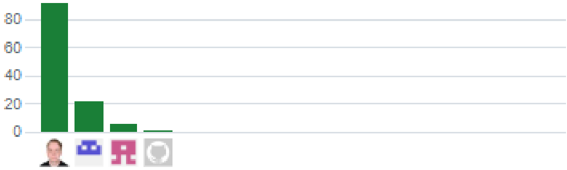
22 commits 587 ++ 164 --



haberturdeur #3

1 commit 168 ++ 3 --

Excluding merges, **4 authors** have pushed **114 commits** to main and **120 commits** to all branches. On main, **30 files** have changed and there have been 7,030 additions and 5,372 deletions.



WRAPPING UP

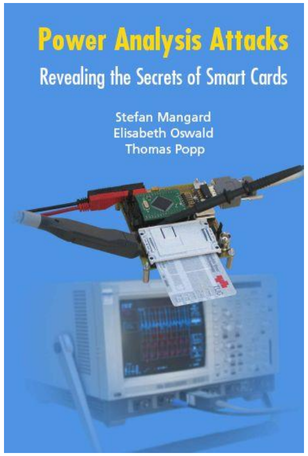
Future Work (for me)

- @ALL: Thank you for your hard work and participation!

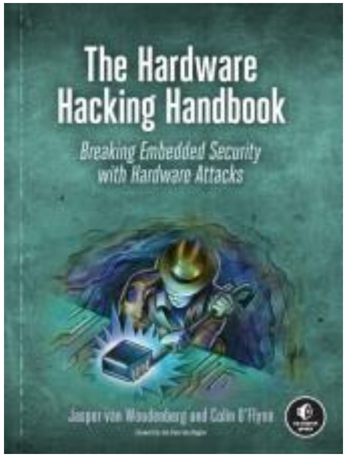
- I would like to use your code in the future to help in the next year’s seminars.
  - Could you make your repositories open-source?
  - Would you like to put the right license?

Still Future Reading

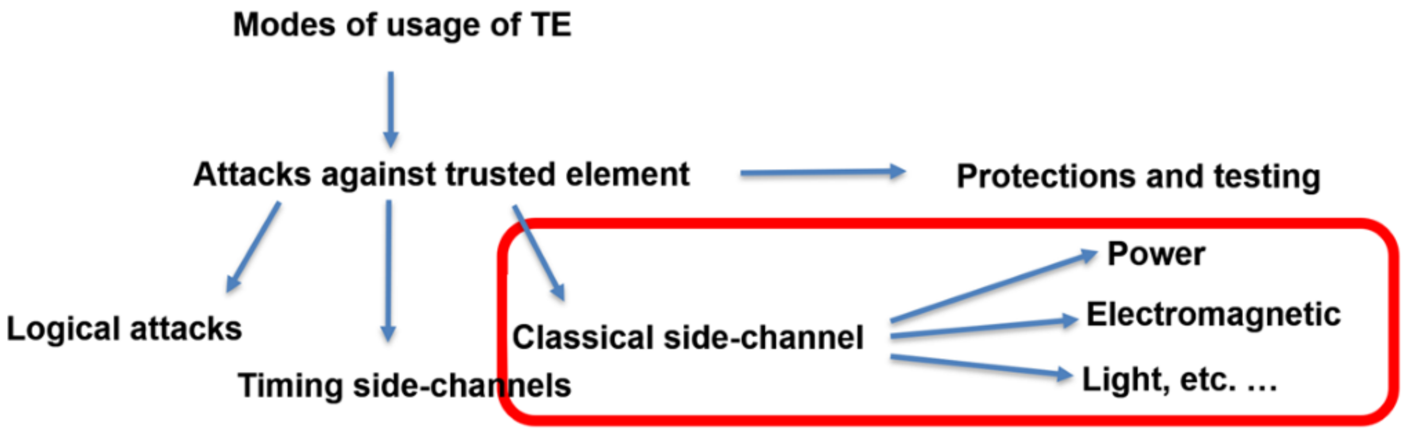
- For interested people
- Side-Channel Analysis – blue book:
  - http://dpabook.iaik.tugraz.at/
  - The books is available at the uni.
  - Look online



- 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

Future Subjects



- PV080 (Information security and cryptography), PV079 (Applied Cryptography), PA018 (Advanced Topics in Information Technology Security)
- PV181 (Laboratory of security and applied cryptography)
- PV286/PA193 (Secure coding principles and practices)
- PV204 (Security Technologies)
- + Bachelor / Master (or even PhD) theses

Thank you very much for attending and for your work!!!

Questions