Toolkit for side-channel analysis SICAK

Petr Socha, Vojtěch Miškovský, Martin Novotný

Czech Technical University in Prague
Faculty of Information Technology
{sochapet,miskovoj,novotnym}@fit.cvut.cz

Jun 24, 2019
Průhonice

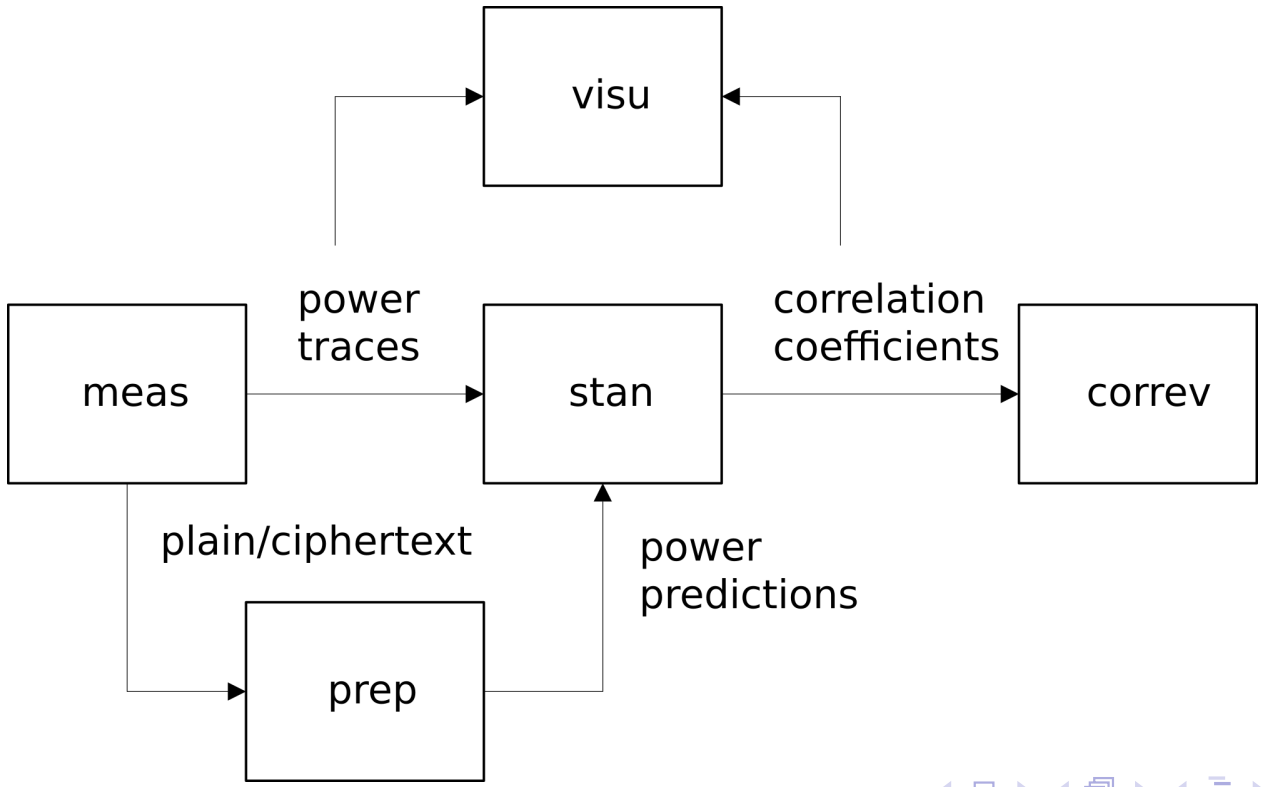
Outline

SICAK - SIde-Channel Analysis toolKit I

- Software toolkit for side-channel analysis
  - active phase - data measurement
  - passive phase - data processing and evaluation
- Set of non-interactive text-based utilities
- Modular plug-in architecture
- C/C++, Qt, qmake
- Multiplatform, tested on Linux and Windows
- Open-source, available on GitHub [1, 2]

SICAK - SIde-Channel Analysis toolKit II

- Currently five utilities:
  - **meas** - Measurement utility
  - **prep** - Data (pre-)processing utility
  - **stan** - Statistical analysis utility
  - **correv** - Correlation attack evaluation utility
  - **visu** - Visualisation utility
- JSON configuration files



Measurement utility (meas)

- Active phase - controlling the device and capturing data
- **Oscilloscope** plug-in
  - Keysight 3000 series (VISA/Linux UsbTMC)
  - PicoScope 6000 series
- **Device Interface** plug-in
  - Serial port
  - SmartCard
- **Measurement Scenario** plug-in
  - Attack (e.g. DPA [3], CPA [4])
  - Test Vector Leakage Assesment [5]

Data (pre-)processing utility (prep)

- Preprocessing power traces
- Preprocessing block data
  - Creation of power predictions based on a power model
    - ★ AES-128 first round S-box Hamming weight
    - ★ AES-128 last round register Hamming distance

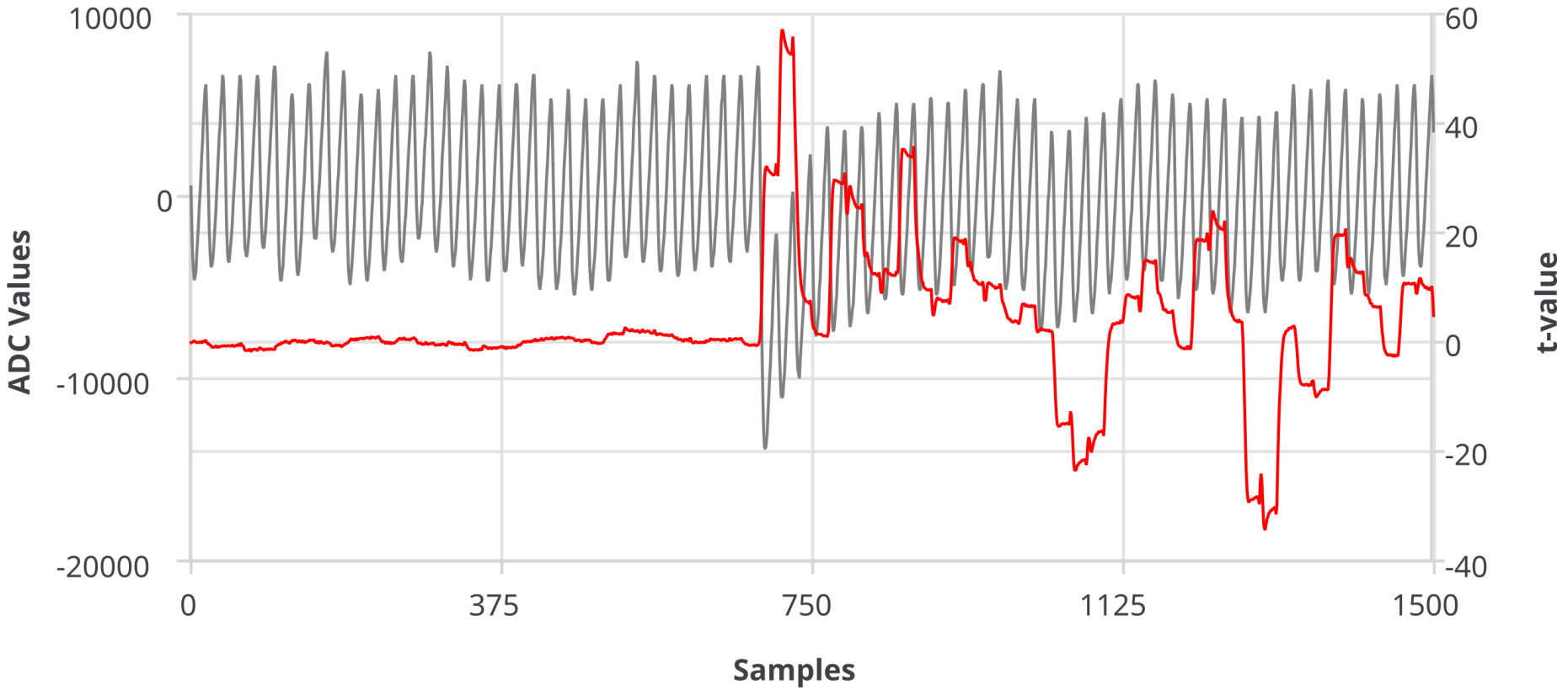
Statistical analysis utility (stan)

- Processing of power traces (power predictions)
- To allow both incremental and iterative computations, three basic functions are implemented:
  - **create** - processes a data set into a statistical context
  - **merge** - merges two existing statistical contexts together (resulting context characterizes union of both data sets)
  - **finalize** - finalizes a context into final results
- Currently implemented plug-in modules include
  - First-order univariate Correlation power analysis [6], accelerated using either OpenMP or OpenCL
  - Arbitrary-order univariate Correlation power analysis [7], accelerated using OpenMP
  - Arbitrary-order univariate Welch's t-test leakage assesment [5]

Correlation evaluation utility (correv)

- Evaluation of CPA correlation matrices
- Different evaluation strategies
  - Minimum/maximum/maximum absolute correlation coefficient
  - Maximum absolute derivative / largest edge [8]
- Different cipher key derivation strategies
  - e.g. last AES round key inversion

Visualisation utility (visu)



Conclusion

- Open-source and multiplatform performance-tuned toolkit for side-channel analysis, written in C/C++
- Modular plug-in based architecture
- Data acquisitions using different measurement scenarios, oscilloscopes and target devices
- Robust, stable and accelerated statistical computations
- Further processing, attack evaluation, and visualisation support
- Non-interactive text-based interface, allowing for scripting usage

References

[1] P. Socha, "Sicak: Side-channel analysis toolkit," GitHub. [Online]. Available: https://petrsocha.github.io/sicak/

[2] P. Socha, V. Miškovský, and M. Novotný, "Sicak: An open-source side-channel analysis toolkit," in *8th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)*, 2019.

[3] P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2004, pp. 16–29.

[5] T. Schneider and A. Moradi, "Leakage assessment methodology," *Journal of Cryptographic Engineering*, vol. 6, no. 2, pp. 85–99, 2016.

[6] P. Socha, V. Miškovský, H. Kubátová, and M. Novotný, "Optimization of pearson correlation coefficient calculation for dpa and comparison of different approaches," in *Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2017 IEEE 20th International Symposium on*. IEEE, 2017, pp. 184–189.

[7] T. Schneider, A. Moradi, and T. Güneysu, "Robust and one-pass parallel computation of correlation-based attacks at arbitrary order," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2016, pp. 199–217.

[8] P. Socha, V. Miškovský, H. Kubátová, and M. Novotný, "Correlation power analysis distinguisher based on the correlation trace derivative," in *2018 21st Euromicro Conference on Digital System Design (DSD)*. IEEE, 2018, pp. 565–568.

Thank you for your attention!

Petr Socha

sochapet@fit.cvut.cz

Acknowledgement: This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency, "Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features" (2016-2018) and CTU project SGS17/017/OHK3/1T/18.