# SICAK: An open-source SIde-Channel Analysis toolKit

Petr Socha, Vojtěch Miškovský, Martin Novotný
Czech Technical University in Prague
Faculty of Information Technology
{sochapet,miskovoj,novotnym}@fit.cvut.cz

**Abstract**

Side-channel cryptanalysis pose a serious threat to many modern cryptographic systems. Typical scenario of a side-channel attack consists of an active phase, where data are acquired, and of an analytical phase, where the data get examined and evaluated.

This work presents a software toolkit which includes support for both phases of the side-channel attack. The toolkit consists of non-interactive text-based utilities with modular plug-in architecture. The measurement utility supports different oscilloscopes, target interfaces and measurement scenarios. The evaluation utilities include support for the test vector leakage assessment and the CPA attack. Different approaches to the algorithmical evaluation of the attack are implemented in order to extract the cipher key. The visualisation utility allows for the visual examination of the attack results by the user.

The toolkit aims to be multiplatform and it is written using C/C++ with performance in mind. Time-demanding operations (such as the statistical analysis) are accelerated using OpenMP and OpenCL for an efficient computation on both CPU and GPU devices.

**Keywords** - Cryptanalysis, Side-channel analysis, Embedded system security, Data acquisition, Statistical analysis

## 1 Introduction

SICAK (SIde-Channel Analysis toolKit) [1] is a set of utilities which aim to offer software support to researchers and scientists in a field of side-channel security. Implementations of many ciphers, even those considered mathematically secure, may leak sensitive information through side channels, such as power consumption. Various side-channel attacks were proposed, e.g. Differential Power analysis [2] or Correlation Power Analysis (CPA) [3, 4], applicable to ciphers such as AES [5], PRESENT [6] or SERPENT [7]. With these attacks on mind, many countermeasures were proposed [8, 9]. To evaluate information leakage of a cryptographic implementation, various leakage

assesment methodologies may be used, and of course, the attack itself may be mounted. This toolkit offers support for both phases of the analysis: the active phase, in which the data are collected, and the analytical phase, in which the collected data are processed and evaluated.

Key features include:

- Written using C/C++ and Qt, supports both **Windows** and **Linux**
- Highly custimizable functionality thanks to **plug-in based** architecture
- Support for **different measurement scenarios** (attack, test vector leakage analysis), using **different target devices** (currently serial/terminal device, SmartCard) and **different oscilloscopes** (currently Keysight 3000 series and PicoScope 6000 series)
- **Arbitrary-order** and **numerically stable** moment-based on-line statistical algorithms (CPA and Welch's t-test), optimized for maximum memory/cache performance and accelerated using OpenMP
- First-order CPA accelerated using OpenCL (GPU); GPU accelerated arbitrary-order analysis hopefully soon to come
- Text-based UI, allowing for scripting usage; JSON configuration files

The toolkit is released under GNU GPLv3 licence and available on GitHub [1].

## 2 Utilities

The toolkit consist of five text-based utilities:

- **meas** - MEASurement utility, which controls the oscilloscope and the device under test (DUT), and manages the data acquisition,
- **prep** - (PRE-)Processing utility, intended for general data processing, e.g. creating power predictions for CPA attack, or preprocessing power traces,
- **stan** - STatistical ANalysis utility, useful e.g. for CPA attack or Welch's t-test analysis,
- **correv** - CORRelation EValuation utility, which provides different strategies for algorithmical evaluation of the correlation-based attack,
- **visu** - VISUalisation utility, useful for plotting power traces, correlation traces or t-values.

These utilities are mostly just empty shells, loading specified plug-ins to define their functionality.

# 3 Plug-ins

The core functionality of the toolkit is found in its plug-in modules. This section contains a summary of currently available plug-ins.

## 3.1 Measurements, Oscilloscopes and Target Devices

Since various tasks require different approaches to the measurement of data, **Measurement Scenario** modules allow for customization of the acquisition procedure. Currently, the attack and the leakage assesment [10] scenarios are implemented.

To allow for usage of different scopes, the meas utility loads an **Oscilloscope** plug-in. Currently, two different oscilloscope modules are implemented: PicoScope 6000 series [11] and Keysight 3000 series [12]. Since the Keysight 3000 oscilloscope module uses standard SCPI commands over VISA/UsbTMC interface, it should work with many other scopes as well, although it is not tested.

Finally, the measurement utility loads a **Target Device** plug-in, which allows control of the DUT using different interfaces. Currently, serial port and SmartCard modules are implemented.

## 3.2 (Pre-)Processing of Data

The preprocessing utility loads a **Traces Preprocessing** or a **Block Data Preprocessing** plug-in module. These allow for a general data processing. Currently, plug-ins for creating power predictions for AES-128 CPA attack are implemented: using Hamming weight when attacking the first round, and using Hamming distance when attacking the last round of the encryption.

## 3.3 Computational plug-ins

These plug-in modules are loaded by the statistical analysis utility. Two different plug-in types exist: attack plug-in (accepting power traces and power predictions), and leakage evaluation plug-in (accepting two sets of power traces).

These modules implement three different operations: "create" context, "merge" contexts and "finalize" context. Given a set of data, these can be processed using the "create" function, resulting in the statistical context (a set of working variables characterizing the statistical moments of the processed data). Two or more context can be merged together, and then finally finalized into the final form (e.g. correlation coefficients in case of CPA attack).

Currently, **first-order** and **arbitrary-order CPA and Welch's t-test** computational plug-ins are implemented. The algorithms are based on formulas present in [13, 10], they are optimized regarding memory and cache

usage, and accelerated on CPU using OpenMP. Furthermore, the first-order CPA attack is accelerated on GPU using OpenCL and available as a separate plug-in module.

### 3.4 Correlation Evaluation plug-ins

To algorithmically evaluate the results of a correlation-based attack, the correlation evaluation utility loads two plug-in modules. A **Correlation Matrix Evaluation** plug-in, which selects a keyguess based on specified characteristics (e.g. maximum correlation coefficient, or a maximum edge on correlation trace [14]), and a **Keyguess Evaluation** plug-in, which may e.g. perform the round key inversion.

## 4 Neat Pictures

In the end, let us present some plots created by the visualisation utility. Figure 1 contains two plots that were obtained while working with the SICAK toolkit. Figure 1a presents 256 correlation traces, with the right key candidate trace highlighted. Figure 1b depicts t-values during an encryption.

## Acknowledgment

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 SGS17/213/OHK3/3T/18.

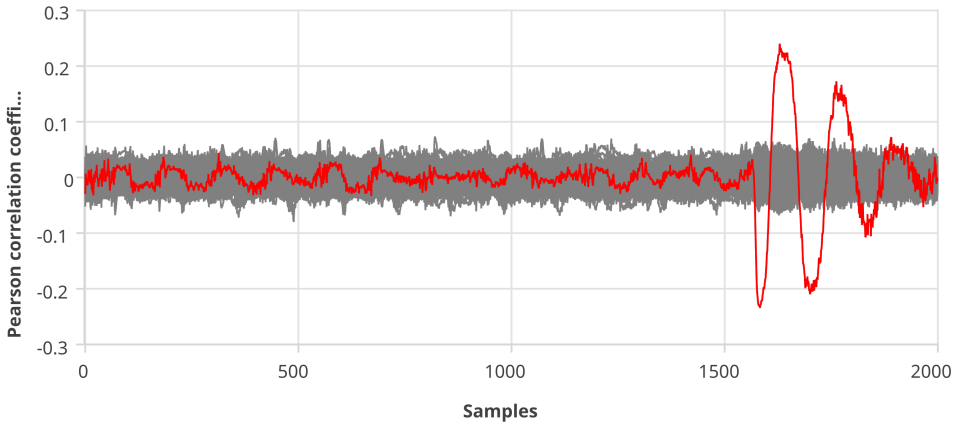
## References

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

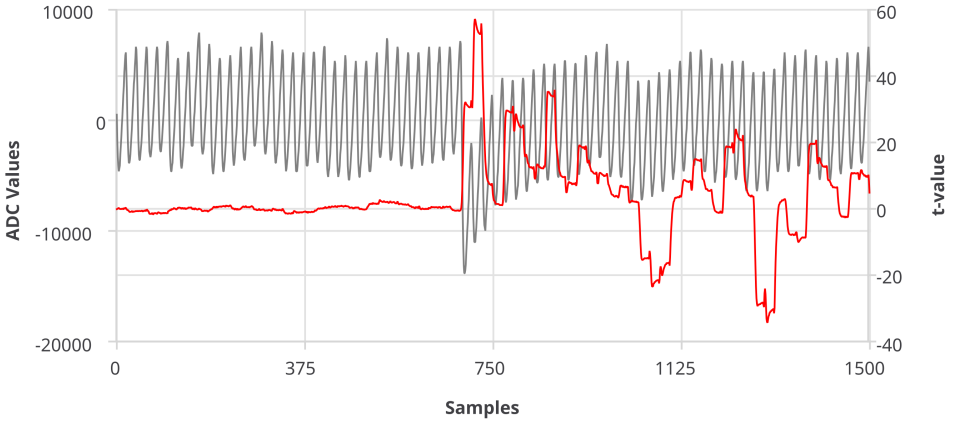
[2] P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[3] B. den Boer, K. Lemke, and G. Wicke, "A dpa attack against the modular reduction within a crt implementation of rsa," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 228–243.

[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.




(a) Correlation traces as a result of the CPA attack




(b) t-values trace and a sample power trace, as a result of the leakage evaluation

Figure 1: Plots created by SICAK VISUalisation utility

[5] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2007, pp. 450–466.

[7] E. Biham, R. Anderson, and L. Knudsen, "Serpent: A new block cipher proposal," in *International Workshop on Fast Software Encryption*. Springer, 1998, pp. 222–238.

[8] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: a very compact and a threshold implementation of aes," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2011, pp. 69–88.

[9] P. Sasdrich, A. Moradi, O. Mischke, and T. Guneysu, "Achieving side-channel protection with dynamic logic reconfiguration on modern fpgas," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2015, pp. 130–136.

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

[11] *PicoScope 6000 Series Programmer's Guide*, Pico Technology Ltd. [Online]. Available: https://www.picotech.com/download/manuals/picoscope-6000-series-programmers-guide.pdf

[12] *Keysight InfiniiVision 3000T X-Series Oscilloscopes Programmer's Guide*, Keysight Technologies, Inc.

[13] 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.

[14] 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.