SICAK: SIde-Channel Analysis toolKit

Petr Socha
Czech Technical University in Prague
Faculty of Information Technology

petr.socha@fit.cvut.cz

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

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 a test vector leakage assessment and a 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 a 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. It is available [1] on GitHub under GNU GPL license.

Acknowledgment

I would like to thank my supervisor Vojtěch Miškovský, and Martin Novotný for their help.

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.

Parts of this thesis were already presented on different occasions: DDECS 2017 [2], DSD 2018 [3], TRUDEVICE 2019 [5] and MECO 2019 [4].

References

[1] Petr Socha. Sicak: Side-channel analysis toolkit. GitHub.

[2] Petr Socha, Vojtěch Miškovský, Hana Kubátová, and Martin 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*, pages 184–189. IEEE, 2017.

[3] Petr Socha, Vojtech Miškovský, Hana Kubátová, and Martin Novotný. Correlation power analysis distinguisher based on the correlation trace derivative. In *2018 21st Euromicro Conference on Digital System Design (DSD)*, pages 565–568. IEEE, 2018.

[4] Petr Socha, Vojtěch Miškovský, and Martin Novotný. First-order and higher-order power analysis: Computational approaches and aspects. In *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–4. IEEE, 2019.

[5] Petr Socha, Vojtěch Miškovský, and Martin Novotný. Sicak: An open-source side-channel analysis toolkit. In *2019 8th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)*, pages 1–4, 2019.