Toolkit for side-channel analysis: SICAK

Petr Socha, Vojtech Miskovsky, Martin Novotny
Czech Technical University in Prague

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.