Security Research Between Attack and Design

Annelie Heuser[1,4], Michael Kasper[2,4], Werner Schindler[3,4], and Marc Stöttinger[1,4]

[1] Technische Universität Darmstadt
Integrated Circuits and Systems Lab
Hochschulstraße 10
64289 Darmstadt, Germany
{Heuser,Stoettinger}@iss.tu-darmstadt.de
[2] Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75
64295 Darmstadt, Germany
Michael.Kasper@sit.fraunhofer.de
[3] Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de
[4] CASED (Center for Advanced Security Research Darmstadt)
Mornewegstraße 32
64289 Darmstadt, Germany
{Annelie.Heuser,Michael.Kasper,Werner.Schindler,Marc.Stoettinger}@cased.de

Abstract

The stochastic approach in power analysis combines engineer's expertise with quantitative stochastic methods from multivariate statistics. Originally, the stochastic approach was developed as an attack tool. Its most important benefit, however, is that it does not only give the information whether an implementation is vulnerable but even quantifies the key-dependent power leakage with regard to a vector space basis.

This feature allows to apply the stochastic approach as a tool to support the design of secure crypto implementations. For instance, imbalanced bit lanes in a particular bus section may be detected, and leakage models can be verified or falsified.

The presentation addresses the different aspects of the stochastic approach from attack to design.