The Stochastic Approach in Power Analysis – An Efficient Attack and Useful Tool for Target-Oriented Design

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

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

Abstract

As template attacks the stochastic approach in power analysis [2, 3] is a profiling-based attack. The stochastic approach combines engineer's expertise with quantitative stochastic methods from the field of multivariate statistics. Unlike in template attacks the designated goal is not the estimation of the exact (unknown) probability distributions, which quantify the leakage, but the estimation of (good) approximators. As a first consequence the profiling workload is by several orders of magnitude smaller than for template attacks while the attacking efficiency is comparable (provided that the designer, resp. evaluator, resp. attacker, has understood the relevant characteristics of the implementation). The attacking efficiency of the stochastic approach is clearly superior to dpa attacks.

The stochastic approach was already presented at CryptArchi 2009. Since then the theory of the stochastic approach has been enhanced in several ways (e.g., PCA could be integrated, allowing to consider a larger number of time instants, thereby easing the task of finding relevant time instants).

Maybe the most relevant advantage of the stochastic approach is that it quantifies the (sub-)key-dependent power leakage with regard to a vector space basis. This property allows to use the stochastic approach as a tool that supports secure design. In our presentation we focus on the connection between side-channel analysis and (re-)design. We present work in progress.

We have investigated the connection between balance properties of bus wires and the β-characteristic, the coefficients with regard to the selected vector space basis. We performed experiments with several AES implementations and different S-box designs on the SASEBO G-I platform [1]. The basis vectors of the 'canonical' 9-dimensional subspace correspond in a straight-forward way to the bit activity of the particular bus lines of the S-box input. The data-dependent load of these bus lines corresponds to the particular β-values. These β-values allow to identify bus lines with higher data-dependent loads (exploitable leakage information) and thereby support the (re-)design of these leaking bus lines. This means that an hardware engineer can use the β-characteristic constructively to identify leaking circuits that are caused by unsymmetrical routing or glitch intensive combinatorial logic.

References

1. http://www.rcis.aist.go.jp/special/SASEBO/index-en.html
2. W. Schindler, K. Lemke, C. Paar: A Stochastic model for Differential Side Channel Analysis. In: J.R. Rao, B. Sunar (eds.): Cryptographic Hardware and Embedded Systems — CHES 2005, Springer, Lecture Notes in Computer Science 3659, Berlin 2005, 30–46.
3. W. Schindler: Advanced Stochastic Methods in Side Channel Analysis on Block Ciphers in the Presence of Masking. Math. Crypt. 2 (2008), 291–310.