Practical vs. theoretical evaluation of DPA and CPA

Annelie Heuser, Sylvain Guilley and Olivier Rioul

TELECOM-ParisTech

Extended Abstract

Different side-channel distinguishers may have different efficiencies, however, their fair comparison is a difficult task, since many factors come into play. In particular, their intrinsic statistical properties and the quality of their estimation are significant factors. Apart from formulating a framework that can be carried out for various distinguishers \cite{8,10}, several works concentrated on the evaluation of the efficiency of certain attacks individually.

More precisely, first works concentrated on finding a link between the Signal-to-noise ratio (SNR) of the power measurements and the effectiveness of the attack. E.g. in \cite{5} the author presents a statistical model for CPA \cite{1}, finding an approximation of the success rate. An extension of this work has been given in \cite{9}. While these works only focused on the correct key guess, Rivain first determined the exact success rate of CPA in \cite{6} assuming an uniform setting in terms of the leakage model.

Recently, Fei et al. introduced a new methodology to evaluate side-channel distinguishers \cite{2} giving the example of DPA \cite{4}. Their approach consists in estimating the success rate of DPA due to the characterization of the physical implementation as well as the cryptographic algorithm. In particular, the authors provided an estimation of the success rate depending on the relationship between the correct and incorrect key hypothesis (named as confusion), the number of measurements and the SNR.

In this talk, we generalize the idea of \cite{2}, that has been restricted to the application of one-bit DPA, to any additive distinguishers and show an application to CPA. Moreover, given the generalized estimation results, we further highlight a new framework to classify distinguishers, which may close the gap between purely practical and purely theoretical evaluations.

References


