Schneider, Tobias; **Moradi, Amir**; **Standaert, François-Xavier**; **Güneysu, Tim**

Bridging the gap: advanced tools for side-channel leakage estimation beyond Gaussian templates and histograms. (English) Zbl 1412.94208

Avanzi, Roberto (ed.) et al., Selected areas in cryptography – SAC 2016. 23rd international conference, St. John's, NL, Canada, August 10–12, 2016. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 10532, 58-78 (2017).

Summary: The accuracy and the fast convergence of a leakage model are both essential components for the efficiency of side-channel analysis. Thus for efficient leakage estimation an evaluator is requested to pick a Probability Density Function (PDF) that constitutes the optimal trade-off between both aspects. In the case of parametric estimation, Gaussian templates are a common choice due to their fast convergence, given that the actual leakages follow a Gaussian distribution (as in the case of an unprotected device). In contrast, histograms and kernel-based estimations are examples for non-parametric estimation that are capable to capture any distribution (even that of a protected device) at a slower convergence rate.

With this work we aim to enlarge the statistical toolbox of a side-channel evaluator by introducing new PDF estimation tools that fill the gap between both extremes. Our tools are designed for parametric estimation and can efficiently characterize leakages up to the fourth statistical moment. We show that such an approach is superior to non-parametric estimators in contexts where key-dependent information in located in one of those moments of the leakage distribution. Furthermore, we successfully demonstrate how to apply our tools for the (worst-case) information-theoretic evaluation on masked implementations with up to four shares, in a profiled attack scenario. We like to remark that this flexibility capturing information from different moments of the leakage PDF can provide very valuable feedback for hardware designers to their task to evaluate the individual and combined criticality of leakages in their (protected) implementations.

For the entire collection see [Zbl 1378.94001].

MSC:

94A60 Cryptography

Full Text: DOI