# Cryptology ePrint Archive: Report 2011/149

**Generic Side-Channel Distinguishers: Improvements and Limitations**

*Nicolas Veyrat-Charvillon and François-Xavier Standaert*

**Abstract:** The goal of generic side-channel distinguishers is to allow key recoveries against any type of implementation, under minimum assumptions on the underlying hardware. Such distinguishers are particularly interesting in view of recent technological advances. Indeed, the traditional leakage models used in side-channel attacks, based on the Hamming weight or distance of the data contained in an implementation, are progressively invalidated by the increased variability in nanoscale electronic devices. In this paper, we consequently provide two contributions related to the application of side-channel analysis against emerging cryptographic implementations. First, we describe a new statistical test that is aimed to be generic and efficient when exploiting high-dimensional leakages. The proposed distinguisher is fully non-parametric. It formulates the leakage distributions using a copula and discriminates keys based on the detection of an ``outlier behavior''. Next, we provide experiments putting forward the limitations of generic side-channel analysis in advanced scenarios, where leaking devices are protected with countermeasures. Our results exhibit that all non-profiled attacks published so far can sometimes give a false sense of security, due to incorrect leakage models. That is, there exists settings in which an implementation is secure against such non-profiled attacks and can be defeated with profiling. This confirms that the evaluations of cryptographic implementations should always consider profiling, as a worst case scenario.

**Category / Keywords:** implementations / side-channel analysis

**Publication Info:** To appear in the proceedings of CRYPTO 2011.

**Date:** received 24 Mar 2011, last revised 30 May 2011

**Contact author:** fstandae at uclouvain be