Countermeasures against EM Analysis

Paolo Maistri, Sébastien Tiran, Amine Dehbaoui,
Philippe Maurine, Jean-Max Dutertre

Abstract

In recent years, side channel analysis has proven to be one of the most dangerous threats to hardware implementation of cryptographic systems, due to its effective trade off between costs and results. After power consumption, electromagnetic (EM) emissions are also becoming attractive, thanks to the fact that the attack can be carried out from a (limited) distance. It is not obvious that countermeasures developed against power analysis are still effective against EM analysis. In this work, we present the results from EM attacks on three different cryptographic implementations, protected against side channel analysis.