Cryptology ePrint Archive: Report 2011/505

A New Second Order Side Channel Attack Based on Linear Regression

Julien Doget and Guillaume Dabosville and Emmanuel Prouff

Abstract: Embedded implementations of cryptographic primitives need protection against Side Channel Analysis. Stochastic attacks, introduced by Schindler et al. at CHES 2005, are an example of such an analysis. They offer a pertinent alternative to template attacks which efficiency is optimal, and they can theoretically defeat any kind of countermeasure including masking. In both template and stochastic attacks, the adversary needs to be able to carry out a profiling stage on a perfect copy of the target device. This makes them interesting tools to study the resistance of implementations against such a powerful adversary, but it limits their pertinency in practice. It is indeed difficult to have an open access to a copy of the device under attack and, even when it is possible, it remains difficult to exploit templates acquired on one device to attack another one. In this paper, we propose a new attack technique which shares many similarities with stochastic attacks but does not require any profiling stage. As a consequence, no copy of the device is needed anymore. We conduct an in-depth analysis of this new attack to highlight its core foundations. Then, we apply it to widely used masking schemes and we illustrate its interest by a series of experiments on simulated and real curves.

Category / Keywords: applications / Side-Channel, Stochastic, Masking, Second-Order, Linear Regression

Date: received 15 Sep 2011, last revised 21 Dec 2011

Contact author: julien doget at gmail com

Available formats: PDF | BibTeX Citation

Version: 20111221:161252 (All versions of this report)

Discussion forum: Show discussion | Start new discussion