Cryptology ePrint Archive: Report 2011/534

Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks

Maxime Nassar and Sylvain Guilley and Jean-Luc Danger

Abstract: Several types of countermeasures against side-channel attacks are known. The one called masking is of great interest since it can be applied to any protocol and/or algorithm, without nonetheless requiring special care at the implementation level. Masking countermeasures are usually studied with the maximal possible entropy for the masks. However, in practice, this requirement can be viewed as too costly. It is thus relevant to study how the security evolves when the number of mask values decreases.

In this article, we study a first-order masking scheme, that makes use of one n-bit mask taking values in a strict subset of $\mathbb{F}_2^n$. For a given entropy budget, we show that the security does depend on the choice of the mask values. More specifically, we explore the space of mask sets that resist first and second-order correlation analysis (CPA and 2O-CPA), using exhaustive search for word size $n \leqslant 5$~bit and a SAT-solver for n up to 8~bit. We notably show that it is possible to protect algorithms against both CPA and 2O-CPA such as AES with only 12 mask values. If the general trend is that more entropy means less leakage, some particular mask subsets can leak less (or on the contrary leak remarkably more). Additionally, we exhibit such mask subsets that allows a minimal leakage.

Category / Keywords: implementation /

Publication Info: Extended version of a paper that will appear at INDOCRYPT'2011

Date: received 30 Sep 2011, last revised 19 Nov 2011

Contact author: sylvain guilley at TELECOM-ParisTech fr