Cryptology ePrint Archive: Report 2011/520

Classification of High-Order Boolean Masking Schemes and Improvements of their Efficiency

Houssem maghebi, Sylvain Guilley, Claude Carlet, Jean-Luc Danger

Abstract: This article provides an in-depth study of high-order (HO) Boolean masking countermeasure against side-channel attacks. We introduce the notion of HO-CPA immunity as a metric to characterize a leakage function. We show that this notion intervenes to assess both the resistance against HO-CPA attacks and the amount of leakage. Namely, the HO-CPA immunity, denoted $\mathsf{HCI} \in \N^*$, coincides with the lowest order of a successful HO-CPA and gives the dependence of leakage behavior with the noise's variance σ^2 (according to $\mathcal{O}(1/\sigma^{2 \times \mathsf{HCI}})$ in Landau notation). Then, we introduce the technique of leakage squeezing. It is an optimization of the straightforward masking where masks are recoded relevantly by bijections. Our main contribution is to show that the HO-CPA immunity of a masking countermeasure can be incremented by one or even by two at virtually no added cost. Indeed, the bijections (and inverse bijections) can be incorporated in tables that are often found in cryptographic algorithms (e.g. substitution boxes).

Category / Keywords: implementation / High-Order Masking, High-Order Correlation Power Analysis (HO-CPA), High-Order CPA Immunity (HCI), Mutual Information Metric (MIM).

Date: received 22 Sep 2011, last revised 26 Sep 2011

Contact author: maghrebi at enst fr