Leakage Squeezing – Defeating Instantaneous $(d+1)$th-order Correlation Power Analysis with Strictly Less Than d Masks

Sylvain Guilley[1], Claude Carlet[2], Houssem Maghrebi[1], Jean-Luc Danger[1], Emmanuel Prouff[3]

[1]TELECOM ParisTech
[2]Univ. Paris 8
[3]ANSSI

Abstract

This talk revisits high-order (HO) Boolean masking countermeasures against side-channel attacks in contexts where the masks are manipulated simultaneously. The relationship between the leakage characteristics and the attack efficiency (Correlation Power Analysis – CPA, and Mutual Information Analysis – MIA) is focused, leading to the introduction of 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. Then, we describe the technique of leakage squeezing. It is an optimization of the straightforward Boolean masking where masks are recoded relevantly by bijections. Our main contribution is to show that this new technique enables to increase the HO-CPA immunity of a masking countermeasure at the cost of a negligible timing/memory overhead.