Cryptology ePrint Archive: Report 2011/056

Spectral Coherence Analysis - First Experimental Results -

Amine Dehbaoui and Sébastien Tiran and Philippe Maurine and François-Xavier Standaert and Nicolas Veyrat-Charvillon

Abstract: This paper introduces a new family of distinguishers for side channel analysis, based on the spectral coherence between leakage traces. Its main goal is to allow adversaries and evaluators of cryptographic devices to take advantage of both time domain and frequency domain intuitions, while also allowing to keep a generic attack in case such intuitions are not available. Compared to previous side channel analysis tools working in the frequency domain, Spectral Coherence Analysis has the significant advantage of directly capturing the degree of similarity between different time domain traces, rather than comparing them with an hypothetical (e.g. Hamming distance) leakage model. In other words, we exploit leakage models to build partitions of the leakage, but not to correlate with an estimated spectrum. As a result, we obtain a more generic and remarkably robust distinguisher. First experiments performed against an unprotected DES implementation suggest that we also gain an improved efficiency in certain meaningful application contexts.

Category / Keywords: Coherence Analysis, SCAN, Side Channel Analysis

Date: received 30 Jan 2011, last revised 30 Jan 2011

Contact author: amine dehbaoui at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110131:044330 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]