Magnitude Squared Coherence based SCA

Sebastien Tiran[(1)], Amine Dehbaoui[(2)], Philippe Maurine[(1)]

[(1)] University of Montpellier / LIRMM
161 Rue Ada
34392 Montpellier France

[(2)] CEA, Centre de Microélectronique de Provence
880, route de Mimet
13541 Gardanne France

Abstract

Many Side-Channel Attacks have been proposed in the literature. Surprisingly, most of them directly work with time domain traces. One obvious drawback of such an approach is the impossibility to capture the complete leakage scattered over many time samples.

Magnitude Squared Coherence is a signal processing tool that indicates how well two time domain signals match one with the other by tracking linear dependencies in their spectral decomposition. It can be used in many ways for Side Channel Analyses. Indeed, if one may use it as a distinguisher, one may also apply it to transform the leakage.

This presentation illustrates and compares different SCA methods based on Magnitude Squared Coherence.