On the use of the EM medium as a fault injection means

Philippe Maurine, Amine Dehbaoui, François Poucheret, Jean-Max Dutertre, Bruno Robisson, Assia Tria

Abstract

The electromagnetic (EM) side channel is a well known source of information leakage. It may be used to conduct passive attacks in order to retrieve sensitive data handled by a secure device.
However, the EM medium may also be used to conduct active attacks. Two kinds of near-field EM perturbations are usually considered: transient pulses and harmonic emissions. We report in this talk our most recent results related to transient pulses. We provide a detailed insight into the use of two different techniques dedicated to the injection of transient faults into a running circuit. Such faults permit us to mount successfully standard differential fault analysis against AES and DES. Fault injection experiments on microcontrollers, FPGA and ASICs will be describe. We also report first explanations on the fault injection mechanism.