Exotic Leakage Models

Moulay Aziz El Aabid, Sylvain Guilley, Jean-Luc Danger
Telecom Paristech, Paris, France

Abstract

High-security devices must be protected against side-channel attacks. Nonetheless, the unintential leakages of some devices can be fairly unexpected in practice. In this presentation, we first illustrate several exotic leakage models (based on real measurements). Then, we discuss several options to detect such leaks as soon as possible in the design flow. Eventually, we advocate that FPGAs are ideal targets to conduct extensive early leakage detection experiments.