The bad and the good of Physical functions

B. Robisson, I. Exurville, H. Le Bouder,
J-M. Dutertre, J. Fournier, J-B. Rigaud

Abstract

Security is a key component of communication and information technology systems: Integrated Circuits (ICs) implementing cryptographic algorithms are used for data confidentiality and integrity or for user/device authentication. Such ICs can be vulnerable to several kinds of attacks. Among them, "hardware attacks", that require a physical access to the circuit, can be used to retrieve cryptographic data (such as "keys") in efficient ways. For example, "observation attacks" consist in observing some physical characteristics (such as the power consumption or electromagnetic radiation) which are modified during an IC's computation. A second family of hardware attacks is that of "perturbation attacks" which consist in corrupting the circuit's behavior. In this presentation, we will first provide formal definitions for leakage functions (i.e. the relationship between the physical characteristics measured during an observation attack and the data manipulated by the circuit) and for error functions (i.e. the relationship between the values of the data which are manipulated by the circuit without perturbations and the corresponding corrupted data generated during a perturbation attack). We shall then illustrate how those formal definitions for leakage functions and error functions can be applied to observation and perturbation attacks on both software and hardware implementations of the AES. Finally we will show how such functions can be used to build schemes for verifying the integrity of integrated circuits.