On the Synthesis of Side-Channel resistant Cryptographic Modules

Sorin A. Huss
Integrated Circuits and Systems Lab
Computer Science Department
Technische Universität Darmstadt, Germany

Abstract — Over the last decades a wealth of computer-aided engineering tools have been conceived and refined in order to significantly shorten the time-to-market in the chip design business in presence of an ever increasing complexity of the design objects. However, up to now, these design support tools still do not provide an efficient HW synthesis-based design strategy for a straight forward engineering of side-channel resistant cryptographic modules.

In order to close this gap, we conceived and developed a novel framework named AMASIVE (Adaptable Modular Autonomous Side-Channel Vulnerability Evaluator). Its purpose is to support a digital circuit designer in implementing side-channel hardened devices by means of an automated design flow. This presentation can be seen as the second of the two contributions, which introduce the AMASIVE framework. While the first one already published in 2012 explains how this software toolset detects automatically vulnerabilities against side-channel attacks in a circuit design, the second one is aimed at an in-depth discussion on how a design of a cryptographic module can be hardened in an automatic way by means of appropriate countermeasures, which are first tailored to the previously identified weaknesses and are subsequently inserted into the initial design by means of a dedicated HW synthesis approach.

In addition to a theoretical introduction of its underlying concepts, we demonstrate a real life application of the AMASIVE toolset to the SCA hardening of the widely used block cipher PRESENT and highlight the resulting effects on an FPGA implementation of this cryptographic module.