Abstract

Mass production and ubiquitous application of integrated logic circuits paved the way for the Digital Revolution and marked the beginning of the Information Age. Novel technologies and information processing devices enabled a plethora of new applications and innovations - ranging from Internet of Things to intelligent transportation systems - that dramatically change our habits and pervade our daily lives. With increasing gain and flow of information, security and privacy is ever becoming more important in particular for nearly ubiquitous small Microcontrollers and embedded devices. Since modern security mechanisms include a lot of complex cryptographic operations that encumber these constrained devices, efficient cryptography on hardware-based accelerators, including Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs), can help to ease this burden. Due to an unhindered and constant physical access and the static behavior and structure of these devices, side-channel attacks are a severe threat to the cryptographic implementations. Consequently, hardware agility, i.e., dynamic structures and constant changes in the circuit and its behavior, will render the static methods of Side-Channel Analysis irrelevant.

The first research contribution of this work is the development of novel low-area and high-performance cryptographic implementations for symmetric and asymmetric cryptosystems on reconfigurable devices. More precisely, this thesis investigates the application of particular features and aspects of modern FPGAs for high-efficient hardware-based cryptography. To this end, this work presents novel applications for Distributed Memory which readdresses configuration memory of FPGAs as user-accessible storage elements in order to design a lightweight AES encryption core. Besides, this thesis at hand demonstrates the application of Block-RAMs and Digital Signal Processors for high-performance implementations of high-security Elliptic Curve Cryptography considered for the next generation of the TLS protocol. To counteract the threat of physical attacks, all presented designs include state-of-the-art side-channel countermeasures which are evaluated under the gray-box adversary model using a practical evaluation setup.

The second contribution of this thesis covers the topic of cryptographic hardware agility for physical protection. In particular, FPGAs as hardware platform for cryptographic accelerations provide the unique feature of run time reconfigurability to load and replace digital circuits on demand. In combination with algorithmic equivalences, the novelty of this work is the application of structural and algorithmic reconfiguration of cryptographic implementations in order to counteract passive Side-Channel Analysis. Consequently, this thesis investigates and evaluates different components of FPGAs that enable the restructuring of hardware circuits. On the path to a generic methodology for circuit reorganization and randomization, the thesis at hand analyzes algorithmic structures for equivalent circuit representations and demonstrates their application for amplification of Threshold Implementations. Eventually, the goal of a generic circuit randomization methodology for viable hardware agility is demonstrated employing the underlying concept and notion of White-Box Cryptography.