Abstract

In recent years, an increasing number of newly-designed products are equipped with small processing devices. Even though these embedded systems are computationally-limited, they are often required to perform complex cryptographic operations to achieve certain security goals, e.g., confidentiality or authenticity. Thus, for these critical and heavy computations, hardware-based accelerators (i.e., Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA)) are utilized to lift the burden from the microprocessor and enable a correct and secure functionality in a constrained environment. Due to their physical accessibility, these cryptographic implementations need to be protected against physical attackers which can passively measure the physical characteristics of the device and actively inject faults in the computation. However, the secure and efficient integration of countermeasures against physical attacks is a non-trivial process, especially for the aforementioned hardware-based accelerators.

The first focus of this thesis is on evaluation methodologies for Side-Channel Analysis (SCA). This passive type of attack has been used in the past to break security-critical embedded systems and poses a severe threat to any unprotected cryptographic implementation. Therefore, the development of countermeasures is of utmost practical relevance. Evaluation methodologies are an essential part of this design process as they represent a valuable tool to assess the vulnerability of a prototype. The results of these evaluations can indicate implementation errors and are used to compare the efficiency of different types of countermeasures. Therefore, they help to significantly improve the final product. There are various different evaluation techniques which can be roughly categorized into attack-based, test-based, and information-theoretic evaluations. This thesis includes contributions to all three categories. In particular, the theory behind the widespread leakage assessment methodology based on Welch’s t-test is extended to allow correct and efficient leakage assessment at higher orders. Furthermore, the computation of correlation-based attacks, which account for a majority of attack-based evaluations, is significantly improved with the introduction of robust and one-pass algorithms to compute Pearson’s correlation coefficient at arbitrary orders. As a third aspect, advanced statistical tools are applied to extend the evaluation capabilities of the information-theoretic metric to enable a more thorough leakage quantification of masked hardware designs. In addition, these tools can be also utilized to improve attack-based evaluation techniques which require density estimation.

The second focus of the thesis is on the design of novel hardware-based countermeasures against physical attacks. Specific physical phenomena, e.g., glitches, make the secure integration of countermeasure, especially masking schemes, on hardware-based devices a challenging process. The concept of Threshold Implementation (TI) represents one solution which enables the design of efficient masked hardware circuits. However, there are still limitations and open problems related to TI. This thesis includes contributions to three unsolved problems of hardware-based countermeasures against physical attacks. For one, the secure conversion between Boolean- and arithmetic-masked values, which has been thoroughly evaluated for software implementations, is examined. In this thesis, the first protected hardware design, which
has been practically verified using the aforementioned leakage assessment methodology, is pro-
polated. Furthermore, the thesis includes a study of cryptographic 8-bit Sboxes which are easy
to protect against side-channel analysis in hardware. To this end, six different 8-bit Sboxes
are presented and form a basis for future research on high-security block ciphers with intrinsic
protection against physical attacks. As a last aspect, a combined countermeasure against both
passive and active attacks is considered. This is a very important problem as secure systems
need to incorporate hybrid countermeasures against both types of physical attacks. However,
the focus of a majority of previous publications lies on only one of these two types of attack,
while excluding the complementary threat. Therefore, the presented construction can be seen
as a foundation which can drive further research in this area.

Keywords.

Physical Attacks, Side-Channel Analysis, Masking, Threshold Implementation, Fault Injection
Attacks, Error-Detecting Codes, t-test, Mutual Information, Pearson’s Correlation Coefficient