The subject of this thesis is the study of symmetric cryptographic primitives. We investigate these objects from three different perspectives: cryptanalysis, design and implementation aspects.

The first part deals with cryptanalysis of symmetric primitives, where one tries to leverage a property of the design to achieve some adversarial goal. Two of the most successful types of cryptanalysis are differential- and linear attacks. We apply variants of differential cryptanalysis to the lightweight block cipher SIMON which was proposed by researchers from the National Security Agency (NSA) in 2013. In particular, we present a search heuristic to find differentials of high probability, and we investigate the clustering of characteristics known as the differential effect. Finally, we apply impossible differential attacks using truncated differentials to a number of SIMON variants. Next, we define a theoretical model for key-less linear distinguishers, which captures the meaning of distinguishing a block cipher from an ideal permutation using linear cryptanalysis, when the key is either known or chosen by the adversary. Such models exist using differential properties but were never before defined using linear cryptanalysis. We apply this model to the standardized block cipher PRESENT. Finally, we present very generic attacks on two authenticated encryption schemes, AVALANCHE and RBS, by pointing out severe design flaws that can be leveraged to fully recover the secret key with very low complexity.

In the second part, we delve into the matter of the various aspects of designing a symmetric cryptographic primitive. We start by considering generalizations of the widely acclaimed Advanced Encryption Standard (AES) block cipher. In particular, our focus is on a component operation in the cipher which permutes parts of the input to obtain dependency between the state bits. With this operation in focus, we give a range of theoretical results, reducing the possible choices for the operation in generalized ciphers to a particular set of classes. We then employ a computer-aided optimization technique to determine the best choices for the operation in terms of resistance towards differential- and linear cryptanalysis. Also in the vein of symmetric primitive design we present PRØST, a new and highly secure permutation. Employing existing third-party modes of operation, we present six proposals based on PRØST for the ongoing CAESAR competition for authenticated encryption with associated data. We describe the design criteria, the usage modes and give proofs of security.

Finally, in the third part, we consider implementation aspects of symmetric cryptography, with focus on high-performance software. In more detail, we analyze and implement modes recommended by the National Institute of Standards and Technology (NIST), as well as authenticated encryption modes from the CAESAR competition, when instantiated with the AES. The data processed in our benchmarking has sizes representative to that of typical Internet traffic. Motivated by a significant improvement to special AES instructions in the most recent microarchitecture from Intel, codenamed Haswell, our implementations are tailored for this platform. Finally, we introduce the comb scheduler which is a low-overhead look-ahead strategy for processing multiple messages in parallel. We show that it significantly increases the throughput for sequential modes of operation especially, but also for parallel modes to a lesser extent.