# Abstract

The research works documented in this thesis lie in the intersection of two different aspects of symmetric key cryptography. From one side the thesis evaluates the security of symmetric-key primitives such as hash functions and authenticated encryption (AE) schemes from the mathematical point of view and from the other side it investigates the physical security of these primitives, notably against fault attacks. For hash functions the cryptanalytic results obtained are on SHA3 standard while the analysis for authenticated ciphers is concentrated on CAESAR candidates. The first part of the thesis highlights a problem that renders differential fault analysis inapplicable to Nonce-based AE. Then it progressively explores three ways to solve the problem leveraging on properties of authenticated ciphers that are often contested to be desirable. The first approach exploits nonce-misuse resistance and onlineness, the second approach exposes the side channel vulnerability of releasing unverified plaintexts while the final approach introduces the notion of fault analysis using internal differentials. Additionally, this part of the thesis reports the first fault analysis of a sponge based mode of operation used in AE and also addresses the problem of fault analysis with partial state information. The second part revolves around finding distinguishers on SHA3 standard and its internal permutation (KECCAK-$p$) which exploit the self-symmetry of the internal state. The first result comes in the form of an interesting property exhibited by a special quartet of coordinates which can be converted to a distinguishing strategy using the internal symmetry of the state. Then it is shown how the technique can be composed with other known strategies to penetrate up to 8 rounds of KECCAK-$p$ using practical query complexities. The second result reports a new distinguishing property of SHA3 hash functions that requires 4 times fewer inputs that the higher-order differential property. It shows and capitalizes on the the existence of special sets of inputs for which the sum of the images under SHA3 exhibits a symmetric property. Interestingly, this work constitutes the first analysis of SHA3/KECCAK that relies on round-constants but is independent of their Hamming-weights. The third part explores the paradigm of guess-and-determine attacks in the context of authenticated encryption. It develops practical key-recovery attacks on CAESAR submission PAEQ in the round-reduced setting. The attacks target the mode of operation along with diffusion inside internal permutation and reach 6,7 and 8 rounds.