In modern cryptography, the security of a cryptosystem is often compromised, not from a theoretical point of view, but by the physical implementation of the cryptographic algorithm. A new class of attacks, called physical attacks, has shown the capability to exploit the unintentional physical behaviors from the cryptographic device, which usually provide enough information to recover the secret keys. In this thesis, various aspects of the physical attacks are covered, with an emphasis on block cipher implementation. We rst investigate different machine learning methods as alternative methods for classical profiling based attacks. Then, machine learning is utilized for the construction of accurate leakage model. Lastly, machine learning is used in combination with profiling side-channel attacks for detection of hardware Trojan. We then provide theoretical fault attacks on LEA block cipher. Then, investigations are done to highlight the practicability of fault attacks, focusing on laser fault injections on smart cards.