Abstract

Fault Attack (FA) is a class of physical attacks where an adversary deliberately perturbs the cryptographic computation and extracts the secret through the faulty system response. The attack techniques in FA vary depending on the type of the faults (called *fault model*), the target algorithm, and the nature of the system response received by the adversary. While equally applicable to both symmetric and public-key paradigms, FAs are widespread in the symmetric-key context, especially for block ciphers. Analyzing state-of-the-art block ciphers in the context of FAs and finding secure design practices for them is a critical, albeit challenging, area of research. Especially, embedded platforms hosting block ciphers allow physical access and multiple attack surfaces to an adversary, making secure design and security testing extremely hard.

The present thesis investigates FA-related security issues in block ciphers with respect to new attacks, their countermeasures, and generic security testing methodologies. It is organized into two parts. In the first part, we propose countermeasures against the Statistical Ineffective Fault Analysis (SIFA), which bypasses most of the existing FA countermeasures proposed so far. Eventually, we figure out a new class of attacks called Fault Template Attack (FTA), which is equally powerful as of SIFA but does not require explicit access to the correct/faulty ciphertexts. The knowledge of whether the ciphertext is correct or faulty is sufficient for key recovery even while the faults are injected at the middle rounds of a block cipher. We also point out why some instantiations of our proposed SIFA countermeasure also work against FTA.

In the second part of the thesis, we address the problem of testing block ciphers and their protected implementations against FA. Two automated frameworks have been proposed in this regard. The first among them is called ExpFault, which automatically identifies exploitable faults in unprotected block cipher algorithms. Additionally, ExpFault also figures out the computational complexity for attacking the algorithm with each exploitable fault. Our second contribution in this regard is a test flow for assessing the FA-induced information leakage from protected block cipher implementation. This leakage assessment methodology, known as DL-FALAT, is based on the theory of *non-interference* and utilizes Deep Learning (DL) for providing a yes/no answer regarding the security of a protected block cipher implementation. DL-FALAT, in principle, bears some similarity with the Test Vector Leakage Assessment (TVLA) methodology for SCA leakage assessment. The efficacy of this proposal is evaluated over a large set of representative countermeasures, including the one proposed by us against SIFA.

Keywords: Fault Attack, Countermeasure, Leakage Assessment, Deep Learning.