Abstract

The SECURITY of BLOCK CIPHERS design are evaluated in two directions: resistance of the cipher against classical cryptanalysis techniques and the other one is the robustness of the cipher against implementation based attacks. Modern day block ciphers are strong against known classical cryptanalytic techniques. However, the implementation based attacks poses a major threat to these ciphers. One such attack is fault based analysis where the secret key of a cipher is retrieved by inducing well defined faults into the hardware implementations of the cipher. In order to develop defence against fault attack, the weakness of the ciphers are to be studied by developing stronger attacks on different type of ciphers. The research focuses on studying the weakness of different block cipher structures against Differential Fault Analysis (DFA) which is more stronger variant of fault attack. Hence, this work first develops DFAs on the internationally standard block cipher Advanced Encryption Standard (AES) which follows a Substitution Permutation Network (SPN) structure. The work develops some of the strongest fault attacks on AES, targeting both datapath and key schedule of AES. Subsequently, the work study the practical feasibility of different fault models used in DFAs. Based on the experimental results on fault injections on hardware design, the work develops state-of-the-art DFAs using multiple byte fault model, which are observed to occur in actual experiments with large probability. The work then studies DFA on standard lightweight block cipher CLEFIA which uses Feistel structure. A new state-of-the-art DFA is developed on CLEFIA which requires least number of faults in existing literature and shows that now ten out of eighteen rounds of CLEFIA need to be protected against DFA. As a next candidate the work then explores a different cipher structure, the AES-finalists block cipher Twofish. It uses key dependent S-boxes and integer modulo addition which make the cipher stronger against differential attacks. The work presents first DFA on Twofish and shows that key dependent S-boxes does not eliminate the threat of DFA. Finally, the work focuses on the threat of DFA to de-

sign of cryptographic hardware specially in the presence of a malicious nexus of multiple parties associated in the different phases of the hardware development. The work designs a stealthy hardware Trojan based on the concept of DFA, which can have catastrophic affect on the cipher implementation when activated by the implanter. In short the thesis studies the weakness of different block cipher structures against DFA and stresses the need for developing suitable countermeasures against DFA. Side by side it opens a new direction of fault tolerant block cipher design based on the cipher structure.

Keywords: Block Cipher, AES, CLEFIA, Twofish, Trojan, Differential Fault Analysis, DFA, Fault Attack, Cipher Structure.