ABSTRACT

Symmetric-key ciphers use the same security-keys for both encryption and decryption. There are two classes of symmetric-key encryption schemes which are commonly distinguished as stream ciphers and block ciphers. Algebraic or statistical analysis mostly target the mathematical strength of the ciphers. Side-Channel Attack (SCA) of stream ciphers is another class of analysis of strength of ciphers, which includes power analysis, timing analysis, etc. Fault attack is one of the most effective forms of implementation attacks against cryptographic algorithms. In this kind of attack, faults are injected during cipher operations. The attacker then analyzes the fault-free and faulty ciphertexts or keystreams to deduce partial or full value of the secret key. Most of the eStream candidates like Grain, MICKEY, Trivium, etc. are vulnerable to fault attacks. Advanced Encryption Standard (AES) is a NIST standard symmetric-key block cipher. AES is also vulnerable to the most powerful Differential Fault Attack (DFA). Designing countermeasures against fault based attack is a challenging task. The thesis investigates for fault resilient Grain-like stream ciphers, and also for fault resilient S-boxes for AES-like block ciphers. The pseudorandom behaviour of Cellular Automata (CA) are used for these research works. The thesis also investigates a new class of nonlinear CA for fault resilient cipher designs. CAESAR: Competition for Authenticated Encryption - Security, Applicability, and Robustness, was started in 2013, which targets to identify a portfolio of authenticated encryption with associated data (AEAD). In literature, there exist some fault attacks on authenticated encryption stream ciphers. AEGIS, a dedicated AES based authenticated encryption algorithm which is a one of the winners of the CAESAR competition, is also susceptible to DFA attack. A variety of countermeasures against fault attacks on AEGIS are proposed here. The thesis also proposes new schemes for generating nonlinear Error Correcting Codes (ECC) using CA, and explores the uses of the codes in designing fault resilient cryptosystems.

Keywords: Symmetric ciphers, eStream ciphers, Grain, AES, Fault Attack, Countermeasures to fault attacks, Cellular Automata