Abstract

Hassan Shokry El-Dib

Synthesis of Fault-Attack Countermeasures for Cryptographic Circuits

Fault attacks are attacks in which an adversary with physical access to a cryptographic device, say a smartcard, tampers with the execution of an algorithm to retrieve secret material. Since the seminal Bellcore attack on modular exponentiation, there has been extensive work to discover new fault attacks against cryptographic schemes and develop countermeasures against such attacks. Originally focused on high-level algorithmic descriptions, these efforts increasingly focus on concrete implementations. While lowering the abstraction level leads to new fault attacks, it also makes their discovery significantly more challenging. In order to face this trend, it is therefore desirable to develop principled, tool-supported approaches that allow a systematic analysis of the security of cryptographic implementations against fault attacks. We propose, implement, and evaluate a new approach for finding fault attacks against cryptographic implementations. Our approach is based on identifying implementation-independent mathematical properties, fault conditions. We choose fault conditions so that it is possible to recover secret data purely by computing on sufficiently many data points that satisfy them. Fault conditions capture the essence of a large number of attacks from the literature, including lattice-based attacks on RSA. Moreover, they provide a basis for discovering automatically new attacks: using fault conditions, we specify the problem of finding faulted implementations as a program synthesis problem. Using a specialized form of program synthesis, we discover multiple faulted attacks on RSA and ECDSA. Several of the attacks found by our tool are new, and of independent interest.