Martin Otto: Fault Attacks and Countermeasures

Doctoral Thesis, 2005, research group “Codes and Cryptography“
Supervisor: Prof. Dr. Johannes Blömer
Department for Computer Science
Faculty for Computer Science, Electrical Engineering, and Mathematics
University of Paderborn

Abstract

This thesis presents new results about fault attacks on cryptographic implementations, as well as new countermeasures against fault attacks. We concentrate on digital signature schemes.
If a cryptosystem is deployed on mobile devices like smartcards, the physical behaviour of the smartcard offers additional sources of information (side-channels, such as timing information or energy consumption). These side-channels can sometimes be used to break cryptosystems, even if those are provably secure in a classical understanding.
This thesis investigates the side-channel given by faulty outputs. There have been two major goals for this thesis: the development of new fault attacks on cryptosystems, and the development of new algorithms, which are secure against fault attacks.
For new fault attacks, we present attacks on the two most popular public key cryptosystems, RSA and elliptic curve cryptosystems. For RSA, we extend a known fault attack on one variant of repeated squaring to the other major variant. Thereby, we show that both variants are equally susceptible to faults. We also investigate fault attacks on repeated doubling used in elliptic curve cryptosystems. Here, we show that contrary to previous believe, fault attacks are not easily defended against. We develop a new fault type and show how this fault type can be used to successfully attack a large variety of variants of repeated doubling.
We also present algorithms, which are secure against known fault attacks. For RSA, we present a new algorithm for CRT-RSA, a fast and the most popular variant of repeated squaring. For elliptic curve cryptosystems, we present a new algorithm for repeated doubling on elliptic curves, which is secure against known and our newly developed fault attacks.