Fault Attacks on Hash-based Signatures (PQ Crypto) (AISEC)

Fault attacks pose a serious threat to embedded systems and their applications. Especially cryptographic algorithms need to be evaluated for any vulnerabilities. However, with the new post-quantum cryptographic algorithms the research of fault attacks is still at its beginning. The Hash-based Signature schemes are particular interesting post-quantum cryptographic algorithms, because they are already rated by NIST as appropriate for use by the U.S. Federal Government. In this work the goal is to understand the existing fault attacks on Hash-based Signatures, and implement & evaluate new possible attack vectors.

The work is designed for a master thesis, but can also be carried out in a limited form within an research or engineering internship.

Prerequisites

Requirements
* Experience with Python
* Basic knowledge in C and Assembly
* Knowledge about Hash-based Signatures is beneficial, but optional
* Experience in FI is beneficial, but optional

Contact

Please send an email with a short CV, your last grading sheet and provide 3-5 dates, which fit to your schedule, for a meeting.

Alexander Wagner, alexander.wagner@aisec.fraunhofer.de

Advisors

Georg Sigl
Alexander Wagner (Fraunhofer AISEC)