TECHNISCHE UNIVERSITÄT DARMSTADT

Master thesis

Analyzing FALCON with respect to side channel and fault attacks

1. General information

Once quantum computers exist, we need post-quantum replacements for the currently used public-key cryptographic schemes. Five families of **post-quantum cryptography** (PQC) exist: Lattice-based cryptography, hash-based cryptography, code-based cryptography, multivariate cryptography, and isogeny-based cryptography.
When it comes to implementing post-quantum cryptography and using it in practical applications, the mathematical security of the schemes is not sufficient, but the **physical security** of the schemes and their implementations, i.e., their resistance towards side channel and fault attacks, has to be ensured as well.
Since most PQC schemes have been developed only recently, not much effort has been put yet into their physical security.

2. Goals

Analysis of the lattice-based signature scheme FALCON (NIST finalist [1]) with respect to its vulnerability to side channel and fault attacks, development of countermeasures.

3. Required skills

The required skills are:

- Course 'Einführung in die Kryptographie' and, ideally, ‚Post-Quantum Cryptography‘
- Good mathematical skills
- Good English skills
- Good programming skills (depending on the concrete research question)
- The thesis should be written in English using LaTeX

4. Contact

If you are interested, please contact: juliane@qpc.tu-darmstadt.de
Dr. Juliane Krämer
S2|20 (CYSEC building)
October 21, 2020

[1] https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions