Invitation to the Oral Examination – Department CE

For the occasion of his examination for a Doctoral Degree,

Thomas Schamberger, M.Sc.

will present his dissertation entitled/on

"Advances of Side-Channel Analysis in the Areals of Post-Quantum Cryptography and Deep Learning-Based Attacks"

on **Wednesday, January 08th, 2025** at **14:00 p.m.**

Attendance to the presentation is open to the public. The presentation will be in English.

The candidate, all members of the Examination Committee, and authorized examiners of the TUM School of CIT are invited to the presentation and subsequent oral examination.

The presentation and subsequent examination will take place in presence at Theresienstr.90, building N1, 1. floor, Room N 1110 A, 80333 München.

Examination committee:

Chair: **Prof. Dr.- Ing. Antonia Wachter-Zeh**

First Examiner: Prof.- Dr. Ing. Georg Sigl

Second Examiner: Prof.- Dr. Ing. Elif Bilge Kavun, Uni Passau

Munich, 20th of December, 2024

Mailing list:

Members of the examination committee

Doctoral candidate

Abstract:

This thesis contributes to the field of Side-Channel Analysis (SCA) with attacks and countermeasures for two post-quantum cryptography algorithms and methods for the explainability of deep learning-based SCA. After an evaluation of making for NTRUEncrypt, the development of chosen-ciphertext attacks and countermeasures for the HQC cryptosystem are presented. Enhancements for the occlusion explainability method are developed based on a comprehensive evaluation of the ASCAD databases.