Bachelor Thesis – Integration of Post-Quantum Schemes into Open Source Internet Applications

Motivation
- A strong quantum computer can break all cryptosystems that are used today in the internet. However, there are cryptographic algorithms, called post-quantum, that are secure against a quantum computer. Integrating these algorithms into everyday applications like e-mail clients or internet browsers is an essential part in keeping IT infrastructures secure.

Goals
- Goal of this thesis is to integrate quantum-secure schemes into open source applications of e-mail clients and/or internet browsers. A Java API providing these schemes is already in development by the UCS working group and should be used in this thesis.

Tasks
- Find open source (Java) applications that make use of cryptographic functions, e.g. e-mail client or internet browser.
- Analyse the applications to see which parts have to be adapted to make use of quantum-safe cryptographic schemes.
- Integrate quantum-safe schemes using the eUCRITE API.
- Evaluate the ease-of-use of the eUCRITE API integration and the performance of the integrated schemes.

Prerequisites
- Good knowledge in IT-security and cryptography.
- Good knowledge of Software-Design.
- Very good knowledge of Java.
- Interest in usability of cryptographic APIs.
- Thesis language can be English or German.

Literature

Start: Right away or by arrangement